Microsoft Windows Server

Microsoft **C**ertified **S**olutions **A**ssociate

گردآورنده:
Payam Avarwand

مقدمه:

وقتی یک شخص، دوره های Network مقدماتی و آشنایی با محیط Windows را با موفقیت پشت سر گذاشته باشد، این کتاب، قدم بعدی، جهت ورود به دنیای حرفه ای شبکه (تحت Microsoft) می باشد.

در روند تهیه ی این کتابچه، بعضی از موضوعات، ناقص باقی ماندند، یا اینکه بطورکلی چیز زیادی در مورد آنها گفته نشده (مثل موضوع PowerShell).

همانطور که احتمالن مشاهده می کنید، این کتابچه دارای دسته بندی های منظم و سلسله مراتبی است که پس از باز کردن آن مثلاً توسط نرم افزار Adobe Reader ، و با باز کردن تب Bookmarks، به سادگی به سرتیترهای این دسته بندی دسترسی خواهید داشت که باعث سرعت عمل در کار با کتاب و دسترسی به موضوعات مختلف آن، خواهد بود.

Practical Glossary:

Phrase / Abbreviation	Meaning	Description
Append	افزودن، ضمیمه کردن	
Appropriate	تخصیص دادن / متناسب، در خور	
Appropriation	تخصیص	
Assign	معین کردن، اختصاص دادن، واگذار کردن	
audit	بازرسی و بررسی کردن	
Availability	در دسترس بودن	
Barebone System	سیستم نیمه آماده	کامپیوتری که فقط شامل قطعات اصلی راه اندازی است.
Built-In	از پیش ساخته شده	
Chip	تراشه	
Credential	مشخصات یک حساب کاربری	به مشخصات یک User که شامل نام و رمزعبور است، گفته می شود.
delegate	محول کردن، وکالت دادن	
Determine	مشخص کردن، معلوم کردن	
DSRM	Directory Services Restore Mode	حالتی که ویندوز Server از Domain جداست. مثل safe Mode
hybrid routing	مسیریابی دو طرفه، ارتباط دوطرفه	
in-house Server	سرور خانگی	
interactive	تعاملی (به شکلی که گفتگو/مذاکره شود.)	
Invoke	فراخواندن، فراخوانی کردن	
Jbod	Just a Bunch of Disks	NRaid or Spanned Raid
Junk Data	داده ی زائد	
Odj	Offline Domain Join	
On premise	Local، در محل	
Platform	بستر، محیط	
Prerequisite	پیش نیاز	
Quota	سهم	
Redundancy	زاپاس داشتن، ذخیره و جایگزین داشتن	
Repository	مخزن	
Statement of work : SOW	شرح کار	
Symmetric	متقارن	
text cursor	نشانگر متن	
to deploy	آماده به کار کردن	
UNC Address	Universal Naming Convention	\\DCName\FolderName
To **power cycle** a device	Turn off and unplug the device and wait at least 30 sec. and plug it in and turn it back on	

1 Bit	0 | 1	
1 Byte	8 Bits	
128 Bytes	1 Kilo Bit	1024 Bits
1 Kilo Byte	1024 Bytes	8 Kilo Bits
1 Mega Byte	1024 Kilo Bytes	1,048,576 Bytes
1 Giga Byte	1024 Mega Bytes	1,073,741,824 Bytes
1 Tera Byte	1024 Giga Bytes	1,048,576 Mega Bytes
1 Peta Byte	1024 Tera Bytes	1,048,576 Giga Bytes
1 Exa Byte	1024 Peta Bytes	1,048,576 Tera Bytes

: Practical Signs

Sign	Name
/	Slash
\	Backslash
|	Pipe
,	comma
:	Colon
;	semicolon
" "	double quotes (quotation marks)
‘ ‘	single quotes
'	Apostrophe
<	left angle bracket
>	right angle bracket
=	equals sign
&	Ampersand
≈	almost equal to
*	Asterisk
@	At Sign
.	Bullet
^	Caret
✓	Checkmark
{	Curly Brackets
}	Left Curly Bracket
°	Degree
¨	Umlaut
÷	Division Sign
-	EN Dash
_	EM Dash
!	Exclamation Mark
♀	Female Sign
½	One half fraction
¼	One Quarter fraction
⅓	One third fraction
¾	Three quarters fraction
>	Greater Than Sign
∞	Infinity
<	Less Than Sign
♂	Male Sign
×	Multiplication Sign
#	Number Sign
Ω	Ohm Sign
(	Parenthese
)	Left Parenthesis
%	Percent Sign
£	Pound Sign
?	Question Mark
"	Quotation Marks
§	Section Sign
[	Square Brackets
]	Left Bracket

Server Hardware :

استفاده از رایانه دسکتاپ یا کیس دار به عنوان **Server** هم امکان پذیر است، اما نه صحیح است و نه عاقلانه است!

اولین نکته در مورد دستگاه های **Server** این است که هیچ گاه خاموش نمی شوند و خاموشی برای **Server** ها معنی ندارد؛ مگر به جهت انجام **Power cycle**، و یا جهت تعویض یا تعمیر قطعات و یا انجام **restart** معمولی جهت طی کردن و تکمیل شدن فرآیندهای نرم افزاری.

برخی طراحی های سخت افزاری در **Server** ها، جهت پایدار ماندن یک **Server**:

- جهت ذخیره سازیِ امن و حفظ و پایداری داده ها، از درگاه های **Hard disk** زیادی پشتیبانی می کنند که آنها را تحت فرآیند قدرتمندی به نام **Raid** همبندی می کنند.
- جهت اطمینان از دریافت و توزیع مناسب جریان برق توسط **Power Supply** میان قطعات، از حداقل دو **PSU** پشتیبانی می کنند.
- جهت خنک نگه داشتن دمای فضای داخلی **Server**، دارای حسگرهایی هستند که با افزایش دما، سرعت چرخش **Fan** های داخل **Server** را افزایش می دهند.
- جهت افزایش و حفظ کارآیی، تعداد زیادی درگاه **RAM** را پشتیبانی می کنند.
- جهت افزایش سرعت در تعویض قطعات سخت افزاری، همه ی **RAM** ها و **PSU** ها، **FAN** ها و **Storage unit** های آنها، قابلیت **hot-swap** را پشتیبانی می کنند و بدون ابزار خاصی و بصورت کشویی، قابل نصب و راه اندازی هستند.
- جهت ادغام شدن کافی در شبکه، دارای چندین **NIC** خواهد بود و چند جای خالی را چند **NIC** های متفاوت نیز پشتیبانی می کنند.

جهت حفظ و پایداریِ جریان برق مصرفی **Server** در صورت قطع برق، دستگاه **UPS** تهیه می کنیم و با آن، **Server** را پشتیبانی می کنیم.

مزیت های کامپیوتر Server نسبت به کامپیوتر معمولی:

- طراحیِ مخصوص برای کار مداوم
- سازگاری قطعات داخلی با یکدیگر
- کارت شبکه قدرتنند
- قابلیت **Hot Swapping**
- قابلیت **RAID**
- دارای **CPU** های قدرتمند زئون (**xeon**) و **Ram** های **ECC** (Error Correcting) هستند.

: Mount the Components

وقتی یک دستگاه Server را خریداری می کنیم، بطورمعمول و پیشفرض:

- برخی قطعات را ندارد، مثل HDD یا SSD ؛ که باید متناسب با دستگاه و از نوع Enterprise Disk تهیه شود.
- برخی قطعات را دارد، اما نه به تعداد کافی، بلکه به تعدادی که بتوان سیستم را روشن کرد، مثل RAM.

نکته:

تمام Disk هایی که برای Server تهیه می شوند، باید دارای مشخصات یکسان باشند.

تمام RAM هایی که برای Server تهیه می شوند، باید دارای مشخصات یکسان باشند.

- همه ی درگاه های RAM، به ترتیب دارای شماره یا حرف (A,B,C,...) هستند، که برای افزودن RAM های جدید به دستگاه، باید به ترتیب درگاه ها را پُر کرد.
- بطور معمول، Server ها حداقل دو درگاه برای CPU دارند، که بطورپیشفرض، خود دستگاه خریداری شده، دارای یک CPU است.
- PSU (Power Supply Unit) های Server شرکت Fujitsu را CSS یا Customer Self Service می گویند، به این معنی که خود مشتری ها هم اجازه ی دریافت و تعویض و جایگذاری آنها را دارند.
- بهتر است که Server حداقل به دو PSU مجهز باشد، تا در صورت بروز ایراد برای PSU فعال، دیگری بطورخودکار جایگزین شود.

:DOM Memory

حافظه های DOM معمولاً برای مکان ها و سازمان هایی که امنیتِ اطلاعات، بسیار اهمیت دارد، استفاده می شوند.

این حافظه ها اطلاعات را به صورت غیر قابل بازگشت ذخیره می کنند و در حجم های پایین (256 MB تا 1 GB) و در 3 نوع 40 Pin ، 44 Pin و SATA تولید می شوند.

شما می توانید اگر Motherboard شما بیش از یک SATA Port دارد، این حافظه های کوچک را مستقیم بر روی Mainboard نصب کرده و اطلاعات حیاتی خود را بر روی آن ذخیره نمایید، تا پس از فروش دستگاه، دیگر نگرانِ بازیابی اطلاعات نباشید.

در هنگام خرید یا استفاده ی حافظه های DOM، باید به نوع نسل آنها و نوع نسل درگاه SATA روی Mainboard نیز دقت کرد.

IPMI (Intelligent Platform Management Interface) :

(درگاه مدیریت هوشمند پلتفورم)

IPMI یک قطعه صفحه chip روی Server است که یک پورت (درگاه) فیزیکی از آن، بر روی Server است که از نوع RJ45 خواهد بود. بطور معمول، در کنار این پورت، یک لوگوی آچار درج شده است، تا از پورت های شبکه، تمایز داشته باشد.

در شرکت های مختلف، این قطعه ای که قابلیت های IPMI را پشتیبانی می کند، با نام های متفاوت شناسایی می شود:

Manufacturer	Software	Description
HP	iLO	Integrated Lights-Out
Dell	iDRAC	Integrated Dell Remote Access Controller
Lenovo	TMM	ThinkServer Management
Fujitsu	iRMC	Integrated Remote Management Controller

قبل از آشنایی با IPMI، ابتدا باید BMC را بشناسیم.

- **«کنترلر بُرد اصلی» یا BMC** (Baseboard Management Controller)**، بوردی سخت افزاری است که به قطعات سخت افزاری اصلی در Server متصل است.**
- **Server می تواند خاموش باشد، اما BMC کماکان آماده ی برقراری ارتباط خواهد ماند، که این قابلیت باعث می شود تا Server بتواند حتی در زمان هایی که خاموش است، همچنان قابلیت نظارت و مدیریت شدن را داشته باشد.**

IPMI به BMC (Baseboard Management Controller) **متصل است.**

برخی ویژگی های IPMI :

- **نظارت بر مشخصه هایی، مثل دما، وضع CPU، حافظه و وضع کلی سیستم**
- **انتقال گزارش های وضعیت از طریق SNMP**
- **روشن و خاموش کردن سیستم Server**

در بعضی سیستم عامل ها، ابزارهایی هم برای کنترل IPMI وجود دارند، مثل IPMI tools یا FreeIPMI.

مهم ترین کاربرد ارتباط توسط این درگاه، دسترسی از راه دور به تنظیمات BIOS دستگاه Server است.

درحقیقت، دسترسی به BIOS یک Server در بستر مخصوص خود iDRAC خواهد بود، که یک محیط تحت وب است.

پس از اتصال Server به شبکه، و تعیین یا اختصاص یک آدرس IP برای محیط iDRAC، به سادگی می توان به تنظیمات BIOS آن Server در هرکجای شبکه، دسترسی داشت.

علاوه بر اینکه هریک از NIC های روی Server یک Mac address مربوط به خود را دارند، خود قطعه ی IMPI نیز یک Mac address مربوط به خودش را دارد.

:(Power Supply Unit) PSU

همانطورکه می دانیم، معمولاً سیستم های **Server** بیش از یک **PSU** دارند، که همگی قابلیت **hot-swap** داشته و بصورت ماژولار و بدون ابزار خاصی (بصورت کشویی)، قابل نصب و استفاده هستند.

- **PSU** (Power Supply Unit) های **Server** شرکت **Fujitsu** را **CSS** (Customer Self Service) می گویند، به این معنی که خود مشتری ها هم اجازه ی دریافت و تعویض و جایگذاری آنها را دارند.
- بهتر است که **Server** حداقل به دو **PSU** مجهز باشد، تا در صورت بروز ایراد برای **PSU** فعال، دیگری بطورخودکار جایگزین شود.
- هر تعداد که **PSU** روی **Server** نصب باشد، همگی باید توسط کابل، به پریز برق متصل باشند؛ تا هرلحظه، آماده ی جایگزینی باشند.
- از نشانه های ایراد و خرابی **PSU** ها:
  - ✓ سروصدای آن، هنگام روشن شدن
  - ✓ بالارفتن دور چرخش **Fan**
  - ✓ خاموشی ناگهانیِ آن
  - ✓ روشن شدن **Server Required LED**
  - ✓ روشن شدن **Fault LED**
  - ✓ روشن نشدن **Server**

: Riser Card

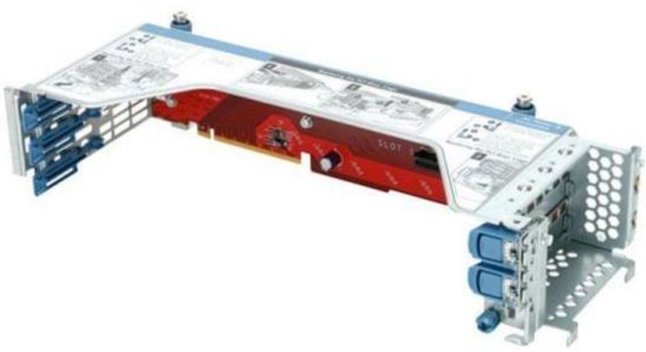
این قطعه، یک نوع مبدل است که معمولاً برای مدیریت فضا بکارگرفته می شود.

در کامپیوترهای معمولی جهت نصب صحیح کارت های گرافیک، و در سیستم های **Server**، برای نصب Raid Controller یا Glass Fiber Controller ها استفاده می شود.

کاربرد آن را می توان به شکل زیر، جمعبندی کرد:

- تبدیل یک درگاه **PCIe** به چند درگاه، جهت افزودن قطعات بیشتر به **Server**
- ایجاد فاصله بین قطعه های سخت افزاری.
- نصب قطعه ی سخت افزاری ای که نیاز به مکان و فضای بزرگتری دارد.
- تغییر حالتِ نصب قطعه ی سخت افزاری روی برد اصلی.





:Raid Controller

اطلاعات پیکربندی مربوط به **Raid Controller**، درون حافظه ای که **Raid Controller Cashe** نام دارد، ذخیره می شوند.
این **Cashe** خیلی نقش حیاتی دارد، چراکه وقتی **Server** خاموش می شود، در صورت خراب یا قطع شدن **Cashe**، کلیه ی تنظیماتی که **Raid Controller** انجام داده بوده است نیز، از دست خواهند رفت. پس **Cashe** باید همیشه روشن و فعال باقی بماند.

به همین جهت، **Raid Controller Cashe**، مجهز به یک باطری است که در صورت قطع برق، حتی تا دو یا سه روز، آن را فعال نگه دارد تا اطلاعات آن از دست نروند.

دو نوع از این باطری ها به شرح زیر هستند:

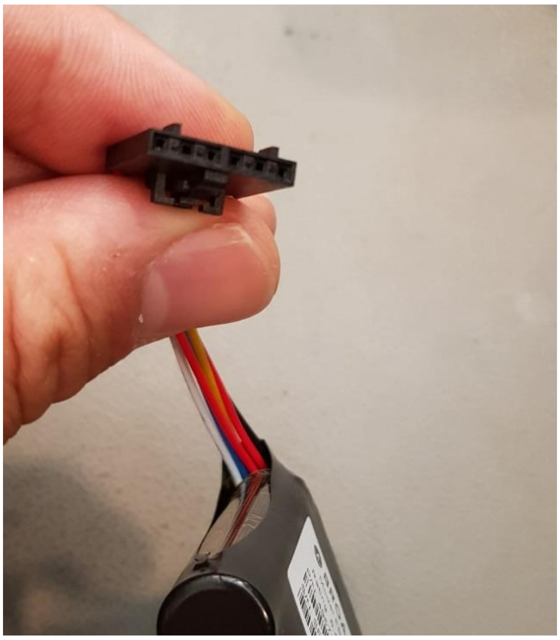
- **BBU** (Battery Backup Unit)
- **FBU** (Flash Backup Unit)

به سبب وجود یک Flash Memory، بهتر و مؤثرتر عمل می کند.



از طرف دیگر، برای کنترل و مدیریت و استفاده ی صحیح از باطری، نیاز به یک **Controller** نیز برای آن داریم، که **TFM Module** نام دارد و بر روی **Raid Controller** نصب شده و فیش باطری را به ورودی آن وصل می کنیم.
در تصویر زیر، **TFM Module** را که روی **Raid Controller** نصب و متصل شده است، می بینید.





- پس نیاز به یک **Riser Card** که دارای حداقل یک **Slot** برای **Raid Controller** و یک جایگاه برای نصب باطری باشد، خواهیم داشت.
- برای جایگذاری باطری روی **Riser Card**، نیاز به یک <u>قاب نگهدارنده</u> خواهیم داشت و برای اتصال فیش باطری به **TFM Module** هم نیاز به یک <u>کابل مجزا</u> داریم.

: Flash Memory

بطور معمول، روی برد اصلی Server ها، روی یکی از درگاه های SATA یک حافظه ی Flash (Flash Memory) قرار دارد، که برای نصب سیستم عامل Server بر روی آن است.تا از حافظه های HDD و SSD بیشترین استفاده را برده و به سادگی از آنها یک RAID Array ایجاد شود.

اما مشکل این SATA Memory سرعت پایین آن است، به همین جهت حداالامکان، سیستم عامل را نیز بر روی بخشی از آرایه ی RAID نصب می کنیم.

Operating System :

بعد از تهیه ی سخت افزار Server، نیاز به یک سیستم عامل می باشد که در این کتابچه با Microsoft Windows Server آشنا می شویم.
در حقیقت شرکت Microsoft دو نوع سیستم عامل دارد:

- Client Operating System : مثل ویندوزهای home edition ، Professional ، Enterprise و ...
- Server Operating System : که آن هم نسخه های متفاوتی دارد.

قبل از تهیه ی یک Windows Server برای دستگاه Server، باید با محدودیت ها و قابلیت های نسخه های موجود آشنا بود.
نسخه های متفاوتی از ویندوز Server وجود دارد مثل:
Standard / Data Center / Essentials / و ...

مشخصه های زیادی در مورد ویندوزهای Server وجود دارد که باید همه ی آنها را با یکدیگر مقایسه کرد، اما مهم ترین ویژگی هایی که باید از ویندوز مورد نظر بررسی کرد و دانست، به شرح زیر می باشند:

- Maximum Number of Users : تعداد User های قابل پشتیبانی در شبکه
- Maximum RAM : بیشترین قدرت و میزان Ram مورد استفاده در سیستم
- Maximum Number of (64-bit) Sockets : تعداد CPU های مورد استفاده در سیستم
- DHCP Server و DNS Server و File Services
- Terminal Services Gateway :

مثلاً برای Windows Server 2016 به شرح زیر می باشد:

Best Offer for RAM : 4 GB
Best Offer for CPU : 2.4 GHz
Best Offer for Hard Disk : 60 GB

نکته ی دیگر در مورد Windows Server 2016 این است که فقط نسخه ی 64 بیتی دارد، و دیگر خبری از 32 بیتی نیست.

پس برای بررسی و مقایسه ی این نسخه با یکدیگر، در google ، جستجو می کنیم: windows server 20xx products and editions

اما نسخه ی کارآمد برای یک Server ، نسخه های Data Center و Standard می باشند.

- WinServer 2016 Data Center : کامل ترین نسخه بوده و تمام قابلیت های Server را پشتیبانی می کند.
  - بر روی بینهایت OSE یا محیط (سیستم) قابل نصب و Implementation است.
  - تا هشت Core CPU را پشتیبانی می کند.یعنی یک CPU «هشت هسته ای» یا دو CPU« چهار هسته ای».
- WinServer 2016 Standard : تنها قابلیت های Virtualisation و Cloud را پشتیبانی نمی کند.
  - بر روی دو OSE قابل نصب و Implementation است.

همانطور که می دانیم، سیستم های Server، سرویس های زیادی را ارائه می دهند، مثلاً Web ، Email، Print ، DHCP و ... .

- اگر یک Server فقط و فقط مسئول یک Service باشد، به آن Dedicated Server گفته می شود.
- اگر یک Server، مسئول بیش از یک Service در شبکه باشد، به آن Non Dedicated گفته می شود.

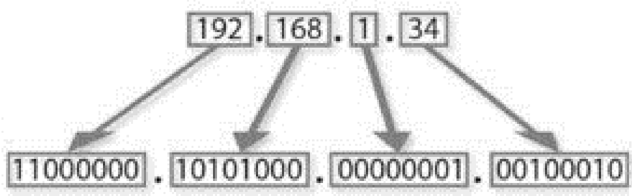
به دلیل هزینه بر بودن Server های Dedicated، معمولاً فقط سرویس های بسیار مهم و سنگین را بصورت dedicated راه اندازی می کنند.

IPv4 :

- هر دستگاه متصل به شبکه، دارای یک آدرس منحصر به فرد است که با مخفف عبارت **Internet Protocol**، یعنی **IP** آن را عنوان می کنند.
- هر **IP** دارای چهار بخش است، که هر بخش می تواند یک عددِ **1** یا **2** و یا **3** رقمی، بین صفر تا 2^8 یعنی **255** باشد، اما چون محدوده اش از عدد صفر شروع می شود، آخرین عدد، **255** در نظر گرفته می شود.
- چون حجم هر یک از این چهار بخش، **8** بیت یا یک **Byte** می باشد، هر بخش را یک **Octet** می گویند.
- پس هر آدرس **IP**، یک آدرس **32** بیتی است.
- هر بخش را با یک نقطه از بخش یا بخش های دیگر جدا می کنند.
- در حقیقت اولین آدرس **IP** به صورت **0.0.0.0** و آخرین آدرس بصورت **255.255.255.255** خواهد بود، که هریک، کاربردهای خاص دارند.
- در حقیقت برای نمایش معمولی **Octet** ها، به شیوه ی **Decimal** عمل می کنیم که رایج و قابل فهم تر است، در صورتی که شیوه ی استفاده ی یک آدرس **IP** در درون سیستم ها، بصورت یک آدرس **Binary** است که شامل هشت بیت است.
- مثلاً آدرس **0.0.0.0** بصورت زیر استفاده می شود:

00000000.00000000.00000000.00000000

مثال:



عدد باینری که اولین بیت سمت راست آن صفر است، حتماً آن عدد، زوج است و اگر بیت سمت راست آن یک باشد، حتماً آن عدد فرد است.
اندیس گذاری هریک از هشت بیتِ یک **Octet** بصورت زیر است:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

همانطور که برای شناسایی هر انسان، یک نام کوچک و یک نام خانوادگی تعیین می شود، بطور مشابه، هر **IP** هم دارای دو بخش است:

- بخش شناسه ی شبکه یا **Network ID**
- بخش شناسه ی میزبان یا **Host ID**

اما اینکه کدام **Octet** یا **Octet** ها را به عنوان **Net ID** و کدام را به عنوان **Host ID** در نظر بگیریم، به این ارتباط دارد که **IP** در چه **Class** ای قرار دارد.

هر آدرس **IP** می تواند در یکی از پنج **Class A** ، **B** ، **C** ، **D** ویا **E** باشد.

: IP classification

در حقیقت، مقدار Octet اول از سمت چپ، همیشه نوع Class را مشخص می کند.
هیچ گاه مقدار Octet اول نمی تواند 00000000 باشد.

: Class A

بزرگترین Class از نظر تعداد آدرس دهی ها، محسوب می شود.
Octet اول از سمت چپ، Net ID و سه Octet دیگر، به ترتیب Host ID محسوب می شوند.

Network	Host		
1 to 126	x	x	x

در Class A، بیتِ اول Octet اول، همواره صفر است.

0XXXXXXX

	7 Bit	24 Bit
0	Network	Host

Class A

در حقیقت آخرین رنج باینری در Net ID این Class، به صورت 01111110 است که برابر با عدد 126 می باشد، و اگر آخرین بیت را هم برابر با یک قرار دهیم، مقدار 127 به دست می آید که البته آن را از مقوله ی classification جدا کرده اند که کاربرد دیگری دارد.

128	64	32	16	8	4	2	1
0	1	1	1	1	1	1	1

➔ ۱۲۷

پس بازه ی تعیین Network برای این Class، از 00000001 تا 011111110 (1 تا 126) می باشد، که می شود : 126
به جز Octet اول، محدوده ی همه ی Octet ها از 0 تا 255 است، و تمام این 256 مقدار، قابل استفاده خواهد بود.
این Class، برای شبکه هایی کاربرد دارد که تعداد میزبان های خیلی زیاد، و تعداد شبکه های کم دارند.
تعداد Host یا همان سیستم های قابل آدرس دهی در این Class 2^{24} عدد است که می شود: 16,777,216
البته در عمل، تعداد Host های قابل آدرس دهی در A Class ، دو عدد کمتر هستند، یعنی 16,777,214 .
همیشه اولین و آخرین آدرس Host، قابلیت دیگری دارند:

1 – 126.0.0.0	آدرس شبکه، یا Network Address
1 – 126.255.255.255	آدرس ارسالات BroadCast

پس اولین آدرسی که در این Class می توان اختصاص داد 1.0.0.1 و آخرین آدرس 126.255.255.254 خواهد بود.

- A Class معمولاً برای موسسات دولتی استفاده می شود.
- از آدرس 127.0.0.1 برای تست سلامتِ کارت شبکه ی سیستم استفاده می شود که به آن Loopback Address گفته می شود.
- آدرسی که نتوان به اعضای شبکه اختصاص داد را آدرس Invalid می گوییم، مثلاً آدرس Network و BroadCast و Loopback همگی آدرس های Invalid هستند.

: Class B

دو Octet اول از سمت چپ، Net ID و دو Octet دیگر، Host ID محسوب می شوند.

Network		Host	
128 to 191	x	x	x

در B Class ، همواره بیت اول و بیت دوم در Octet اول، به ترتیب یک و صفر هستند.

10XXXXXX

پس در Octet اول این Class، فقط 6 بیت متغیر داریم، که بازه ی آن از 10000000 تا 10111111 می باشد.

پس تعداد Network هایی که در این Class می توان تعیین کرد، برابر است با 2-216 یا 16,384 عدد

تعداد Host یا همان سیستم های قابل آدرس دهی در این Class 216 عدد منهای 2 است که می شود : 65,534 عدد.

16	16	
Network	Host	**Class B**

128 – 191.0.0.0	آدرس شبکه یا Network Address
128 – 191.255.255.255	آدرس BroadCast

پس اولین آدرسی که در این Class می توان اختصاص داد 128.0.0.1 و آخرین آدرس 191.255.255.254 خواهد بود.

: Class C

سه Octet اول از سمت چپ، Net ID و تنها Octet سمت راست، Host ID محسوب می شود.

Network			Host
192 to 223	x	x	x

در C Class ، همواره بیت اول و دوم و سوم در Octet اول، به ترتیب یک و یک و صفر هستند.

110XXXXX

پس در Octet اول این Class، فقط 5 بیت متغیر داریم، که بازه ی آن از 11000000 تا 11011111 می باشد.

پس تعداد Network هایی که در این Class می توان تعیین کرد، برابر است با 3-224 یا 2,097,152 عدد .

تعداد Host یا سیستم های قابل آدرس دهی در این Class، دو به توان 8 عدد، منهای 2 است که می شود : 254 عدد.

24	8
Network	Host

192 – 223.0.0.0	آدرس شبکه، یا همان Gateway Address
192 – 223.255.255.255	آدرس BroadCast

پس اولین آدرسی که در این Class می توان اختصاص داد 192.0.0.1 و آخرین آدرس 223.255.255.254 خواهد بود.

Class D :

Network	Host		
224 to 239	x	x	x

در D Class ، همواره چهار بیت اول در Octet اول، به صورت 1110 هستند.

1110XXXX

پس در Octet اول این Class، فقط 4 بیت متغیر داریم، که بازه ی آن از 11100000 تا 11101111 می باشد.

از آنجایی که از این Class برای Multicasting استفاده می شود، Net ID و Host ID برای این Class بی معنی است.

جهت استفاده های Multicast بکار می رود.

Class E :

Network	Host		
240 to 254	x	x	x

در E Class ، همواره چهار بیت اول در Octet اول، به صورت 1111 هستند.

1111XXXX

پس در Octet اول این Class هم فقط 4 بیت متغیر داریم، که بازه ی آن از 11110000 تا 11111111 می باشد.

این Class برای کار های تحقیقاتی و تجربی محیا شده است و ما نمی توانیم از این آدرس استفاده کنیم، به همین دلیل به این Class، Experimental گفته می شود.

Public / Private :

در هر **Class**، دو نوع **IP Address** موجود می باشد:

Private address :

برای استفاده در شبکه های **Local** استفاده می شود و برای استفاده از آنها احتیاج به هیچ مجوزی نیست؛ چون در **Router** ها به بیرون شبکه، مسیریابی نمی شوند.

Public address :

هر **Public Address**، یک آدرس یکتا یا **Unique** است که یک آدرس عمومی و معتبر در فضای اینترنت محسوب می شود.
سازمانی که **Public IP** ها را مدیریت و کنترل می کند، سازمان **IANA** (Internet Assigned Numbers Authority) است.
پس جهت دریافت یک **Public IP**، لازم است که از سازمان **IANA** مجوز دریافت کرد.

برای تشخیص اینکه یک **IP** عمومی است یا خصوصی، تعدادی از آدرس ها را به شکل استاندارد، به عنوان **Private IP**، تعیین کرده اند که آنها را برای سه کلاس **A** و **B** و **C** جدا و تعریف کرده اند.
پس اگر یک **IP** در این بازه ها باشد، خصوصی است، در غیر اینصورت عمومی است.

Class	Beginn	End
A	**10**.0.0.0	**10**.255.255.255
B	**172.16**.0.0	**172.16**.255.255
C	**192.168**.0.0	**192.168**.255.255

: Range Analysis

:Example1

شبکه ای که آدرس 130.64.33.25 در آن وجود دارد را تحلیل کنید.

از آنجایی که 130 در محدوده ی Class B قرار دارد:

Class	B
Network ID	**130.64.0.0**
First valid IP Address	**130.64.0.1**
Last valid IP Address	**130.64.255.254**
BroadCast Address	**130.64.0.255 _ 130.64.255.255**
Number of Availabe IP Addresses	**2^{16} = 65536**
Number of valid IP Addresses	**2^{16} -2 = 65534**

:Example2

فرض کنیم در شبکه ای 200 عضو وجود دارند، از کدام Class استفاده کنیم؟

پس باید شرط زیر برقرار باشد:

$$2^{(\text{تعداد بیت های Host})} >= 200$$

$Log_2 200 \sim 7.6 = 8$ تعداد بیت های Host

نکته: از آنجایی که در همه ی ماشین حساب ها، بطور پیشفرض، لگاریتم همه ی اعداد در مبنای 10 حساب محاسبه می شود، و در بیشتر آنها قابلیت دریافت لگاریتم یک عدد در مبناهای دیگر مقدور نیست، می توان از ln کمک گرفت.

مثلاً پاسخ Example بالا را می توان در ماشین حساب بصورت زیر بدست آورد:

ln(200) ÷ ln(2) = 7.6

قوانین و فرمول‌های لگاریتم :

لگاریتم هر عدد در پایه ی خودش، برابر است با یک. $log_x x = 1$

لگاریتم یک، در پایه ی هر عدد، برابر است با صفر. $log_a 1 = 0$

لگاریتم حاصل ضرب دو عدد برابر است با جمع لگاریتم هر کدام از آنها. $log_a xy = log_a x + log_a y$

لگاریتم تقسیم دو عدد برابر است با لگاریتم عدد صورت منهای لگاریتم عدد مخرج. $log_a \frac{x}{y} = log_a x - log_a y$

در صورتی که عدد جلوی لگاریتم به توان برسد، می‌توان توان را به پشت لگاریتم برد و در آن ضرب کرد. $log_a x^n = n log_a x$

پس، از آنجا که در Class C تعداد بیت های Host هشت است، Class این شبکه را، C در نظر می گیریم، که تا 255 آدرس را پشتیبانی می کند.

Network	Host
xxxxxxxx.xxxxxxxx.xxxxxxxx	hhhhhhhh

:Example3

آیا آدرس های 80.81.26.50 و 80.83.15.44 در یک شبکه قرار دارند؟

ابتدا Class آنها را پیدا کرده و سپس محدوده های Net ID و Host ID را پیدا می کنیم.

Network	Host		
80	81	26	50

Network	Host		
80	83	15	44

با توجه به اینکه هر دو در A Class قرار دارند و هر دو دارای Net ID یکسان هستند، پس در یک شبکه قرار دارند.

80.81.26.50
80.83.15.44

:Example4

آیا آدرس های 194.167.32.0 و 194.167.33.0 در یک شبکه قرار دارند؟

با توجه به اینکه هردو در Class C قرار دارند، و دارای octet سوم متفاوت هستند، پس Net ID یکسانی ندارند، پس در یک شبکه نیستند.

194.167.33.0
194.167.32.0

Subnet Address :

برای اینکه برای یک کامپیوتر مشخص شود که تا کجای یک آدرس IP مربوط به Net ID و از کجا به بعد مربوط به Host ID است، از یک آدرس دوم استفاده می کنیم به نام Subnet Mask.

دو الگو برای subnet mask وجود دارد:

❖ **الگوی Standard یا Classfull:**

با توجه به Class ای که IP در آن قرار دارد، یک subnet mask استاندارد برای آن IP داریم:

Class A	255.0.0.0	11111111.0000000.00000000.0000000
Class B	255.255.0.0	11111111.11111111.00000000.0000000
Class C	255.255.255.0	11111111.11111111.11111111.0000000

- قسمتی که 255 است متعلق به network و قسمتی که 0 است متعلق به host می باشد.
- در حقیقت کامپیوتر از طریق And کردن بیت های Subnet mask با بیت های آدرس IP، Network ID را بدست می آورد.
- به این نوع الگوبندی برای Subnet Mask ، Subnet mask format نیز گفته می شود.
- در بیشتر شبکه های خانگی یا کسب و کارهای کوچک، چون آدرس دهی در Class C است، آدرس زیرشبکه، 255.255.255.0 می باشد.

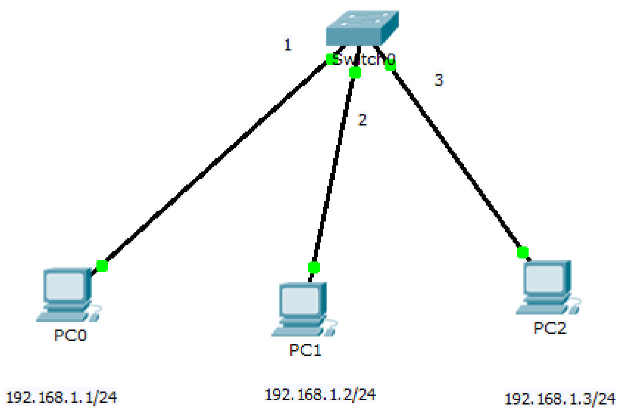
❖ **الگوی Non-standard یا Classless Address :**

الگوهایی هستند که دقیقاً با محدودیتهای هشت بیتی، مطابقت نمی کنند، چون برای نیازهای خاصی طراحی شده اند.

به این نوع الگوبندی برای Subnet Mask ، Prefix format نیز گفته می شود.

می توانیم به سادگی بعد از درج آدرس IP، یک علامت / درج کنیم، و سپس با درج تعداد بیتهای NET ID، subnet mask آن IP را مشخص کنیم.
به این عدد، Prefix Notation یا Net Mask گفته می شود.

مثال: در آدرس 192.168.1.2/24 متوجه می شویم که تمام بیت های سه Octet اول در Subnet mask ، یک هستند، و فقط مجاز به استفاده از 8 بیت برای آدرس دهی Host ها هستیم.
مثال: در شکل زیر سه کامپیوتر داریم که همخانواده و در کلاس C هستند، چون Net ID آنها مشترک است:



:Wildcard mask

می دانیم که هر آدرس IP دارای یک آدرس Subnet mask نیز می باشد، که به ازای بخش ثابت آن آدرس IP، در Subnet mask عدد 255 درج می شود.
که در حقیقت در هر Octet، برای نمایش عدد 255، هشت عدد 1 درج خواهد شد.

از آنجایی که در برخی سیستم ها و دستگاه ها، بررسی و چک کردن اعداد صفر، سریع تر از عدد یک می باشد، مفهومی تعیین شد به نام Wildcard mask، که نسخه ی عکس Subnet mask می باشد.
مثلاً نسخه ی Wildcard mask برای یک آدرس کلاس C، می شود: 0.0.0.255

برای بدست آوردن Wildcard یک آدرس IP، کافی ست آدرس 255.255.255.255 را منهای آدرس Subnet mask آن کنیم.

مثلاً wildcard address برای 255.255.255.128 برابر است با: 0.0.0.127

مثلاً wildcard address برای 255.255.252.0 برابر است با: 0.0.3.255

VLSM (Variable Length Subnet Mask) :

فرض کنید شما یک مهمانی برگزار کرده اید و می دانید که حداکثر مهمان های شما 200 نفر هستند.
پس 200 کارت دعوت چاپ می کنید.
هر کس که یکی از این کارت های دعوت را داشته باشد، می تواند در مهمانی شما شرکت کند و پذیرایی شود.
اما در نظر بگیرید که مهمان های شما همان 200 نفر هستند، اما شما 800 کارت دعوت چاپ کرده اید.چه اتفاقی می افتد؟
در خوشبینانه ترین حالت، هیچ اتفاقی.
اما در حالت غیر خوشبینانه، اگر فرد یا افراد غریبه ای به این کارت های دعوت دسترسی بیابند می توانند در مهمانی شما شرکت کنند و همه ی شیرینی ها را بخورند!!!

ایجاد زیرشبکه در سه حالت و به دو شکل انجام می شود:

- اگر تعداد کل Host ها از میزان Host ID به مقدار قابل توجهی، کمتر باشد.

با قرض دادن تعدادی بیت از قسمت Host به قسمت Network صورت می گیرد، که به این عمل، **Supernetting** گفته می شود.

- اگر تعداد کل Host ها زیادتر از میزان Host ID باشد:

با قرض گرفتن یک یا تعدادی بیت از قسمت Net ID و اضافه کردن به Host ID صورت می گیرد، که به این عمل، **Subnetting** گفته می شود.

- از طرف دیگر، Subnetting یا Supernetting را در زمانی که بخواهیم یک محدوده ی IP را برای چند شبکه ی متصل به هم، استفاده کنیم نیز استفاده می کنیم، که این حالت، در مواقعی از قبیل زیر ضروری است:
  - ✓ شرکت یا سازمان از تکنولوژی های مختلف، چند اتصال Client ها به شبکه استفاده می کنند. (Ethernet ، wireless و یا ...)
  - ✓ دو یا چند بخش از شبکه در محدوده های جغرافیایی مختلفی قرار گرفته اند.
  - ✓ برای اینکه بتوانیم بخش های مختلف شبکه را متمرکزسازی (Centralization) کنیم. (قسمت مالی، قسمت آموزش و ...)
  - ✓ کامپیوترهایی که نیاز به Bandwidth بیشتری در شبکه دارند، می بایست از دیگران مجزا شوند.

پس زمانی که یک محدوده ی آدرس دهی را به تعدادی محدوده ی کوچکتر شکسته و تقسیم بندی کنیم، هر یک از رنج های شکسته شده، یک زیرشبکه است.

مزایا و معایت Subnetting و Supernetting :

- امنیت شبکه را بیشتر می کند.
- به شما انعطاف پذیری و قدرت مانور بیشتری در تعیین آدرس ها در شبکه می دهد.
- باعث مدیریت آسانتر شبکه می شود.
- جهت وقوع اشکال در شبکه، سرعت عیب یابی بیشتر خواهد بود.
- باعث می شود که اندازه ی جدول های مسیریابی (Routing Table) در Router ها کاهش پیدا کند.
- فرآیند مسیریابی بهتر و سریع تر خواهد بود.

از آنجایی تحت این دو فرآیند، آدرس Subnet از حالت standard یا Classfull خارج می شود، به این دو روش، **CIDR** (Classless Inter-DomainRouting) گفته می شود.

چرا به جای Subnetting، به سادگی از آدرس های مختلف استفاده نکنیم؟

این دو حالت را در نظر بگیرید:

- **DHCP داشته باشیم.**

اگر DHCP داشته باشیم و شما بخواهید برای هر واحد، رنج IP جدا در نظر بگیرید، در این صورت:

  - به ازای هر واحد باید یک Scope جدید در DHCP تعریف کنید.
  - به ازای هر Scope در DHCP باید یک کارت شبکه ی جدا داشته باشید.
  - به ازای هر کامپیوتر باید Reservation در DHCP انجام دهید و یا هر کارت شبکه مستقیما به واحد مربوطه وصل شود و آن واحد هم باید از لحاظ فیزیکی ایزوله باشد وگرنه در شبکه هرج و مرج بوجود می آید.

- **DHCP نداشته باشیم.**
  - باید برای هر واحد به صورت دستی IP ها را Set کنیم.
  - اگر یک روز دستور بیاید که همه با هم شبکه شوند، دوباره کلی IP هست که باید تغییر داد! در حالی که با استفاده از Subnetting فقط باید Subnet mask را تغییر داد.

The amount of Net masks :

یادآوری فوری مقادیر Subnet mask ها با توجه به مقدار net mask آنها:

10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

:Example1

فرض کنید در یک سازمان، یک شبکه ی بزرگ با 5000 کامپیوتر داریم و می خواهیم آنها را شبکه کنیم، و از قبل، IP زیر به عنوان **Network Address** تعریف شده است:

165.12.0.0 /16

همانطور که پیداست، این IP در **B Class** قرار دارد، با یک **Prefix Notation** استاندارد یا **Classfull**.

- با توجه به اینکه می دانیم با این آدرس در این **Class** تا **65,534** کامپیوتر را می توانیم آدرس دهی کنیم، پس حالت **Classfull** مفید نیست، چون تعداد خیلی زیادی آدرس، بی استفاده خواهند ماند؛ و باید آدرس های موجود را تا حد زیادی کاهش دهیم.
- مجبور به قرض دادن تعدادی بیت از محدوده ی **Host ID** به **Net ID** خواهیم بود. (**Classless**)

به عملیاتی که به بیت های Net ID افزوده می شود، Supernetting گفته می شود.

روش اول:

ابتدا آدرس **IP** را بصورت بیتی درج می کنیم:

10100101.00001100.00000000.00000000

تعداد آدرس های موجود : $2^{16} - 2 = 65,534$

سعی می کنیم میزان بیت های **Host ID** را با قرض دادن مثلاً دو بیت به **Net ID** حساب کنیم:

10100101.00001100.00000000.00000000

$2^{16-2} - 2 = 16,382$

هنوز مقدار **Host ID**، عدد بزرگی برای آدرس دهی 5000 کامپیوتر است، پس یک بیت دیگر از آن را قرض می دهیم:

$2^{16-3} - 2 = 8,190$

پس با تحویل سه بیت از **Host ID** به **Net ID** ، به سادگی خواهیم توانست 5000 کامپیوتر را با یک **B Class IP**، آدرس دهی کنیم.

روش دوم:

$\mathrm{Log}_2\, 5000 \sim 12.28 = 13$ تعداد بیت های Host

پس آدرس **IP** به صورت زیر در خواهد آمد:

10100101.00001100.00000000.00000000
165.12.0.0/19

آدرس **Subnet mask** نیز به صورت زیر در خواهد آمد:

11111111.11111111.11100000.00000000

128	192	224	240	248	252	254	255
1	1	1	0	0	0	0	0

255.255.224.0

- پس **8,190** آدرس موجود خواهد بود، طوری که هر **255** آدرس به هریک از زیرشبکه ها، اختصاص می یابد.

برای اینکه تعداد زیرشبکه ها را بدانیم، کافی ست که دقت کنیم که در **Octet** دستکاری شده، **5** بیت مختص **Host ID** می باشد، پس دو را به توان این **5** می رسانیم که می شود : **32** .

پس **32** زیر شبکه خواهیم داشت، که به صورت زیر خواهند بود:

165.12.0.0	til	165.12.0.255	for 255 Host
165.12.1.0	til	165.12.1.255	for 255 Host
165.12.2.0	til	165.12.2.255	for 255 Host
165.12.3.0	til	165.12.3.255	for 255 Host
…	…	…	…
165.12.31.0	til	165.12.31.255	for 255 Host

برای نمایش محدوده ی این شبکه بصورت کاملاً خلاصه:

165.12.0.0 - 165.12.31.255

:Example2

فرض کنید در یک سازمان، یک شبکه ی بزرگ با 700 کامپیوتر داریم و می خواهیم آنها را شبکه کنیم، و از قبل، IP زیر به عنوان Network Address تعریف شده است:

194.167.32.0 /16

همانطور که پیداست، این IP در کلاس C قرار دارد، با یک Prefix Notation استاندارد یا Classfull.

می دانیم در این Class فقط تا 254 کامپیوتر را می توانیم آدرس دهی کنیم، پس میزان Host ID کفایت نمی کند!
پس مجبور به قرض گرفتن تعدادی بیت از محدوده ی Net ID خواهیم بود، تا به شکل Classless آدرس دهی را انجام دهیم.
پس به عملیاتی که انجام خواهیم داد، Subnetting گفته می شود.
ابتدا آدرس IP را بصورت بیتی درج می کنیم:

11000010.10100111.00100000.00000000

$$2^8 - 2 = 254$$

سعی می کنیم میزان بیت های Host ID را در صورت قرض گرفتن یک بیت از Net ID حساب کنیم:

11000010.10100111.00100000.00000000

$$2^{8+1} - 2 = 510$$

خب هنوز هم نیاز ما برای آدرس دهی 700 کامپیوتر را رفع نمی کند، پس دو بیت قرض می کنیم:

$$2^{8+2} - 2 = 1022$$

پس با تحویل دو بیت از Net ID به Host ID ، به سادگی خواهیم توانست بیش از 700 کامپیوتر را آدرس دهی کنیم.
آدرس IP به صورت زیر در خواهد آمد:

11000010.10100111.00100000.00000000
194.167.32.0/22

البته می توانستیم در همان ابتدا تعداد بیت های Host را به صورت Log2700 محاسبه کنیم: .. ln(5000)÷ln(2) ~ 9.
و تعداد بیت ها را 10 در نظر می گرفتیم.

آدرس Subnet mask نیز به صورت زیر در خواهد آمد:

255.255.252.0

11111111.11111111.11111100.00000000

پس IP بصورت 194.167.32.0/22 در خواهد آمد.
پس برای 1024 آدرس، باید این مقدار را در زیرشبکه ها به شکل هر 255 آدرس در هر یک زیرشبکه، تقسیم کنیم.
برای اینکه تعداد زیرشبکه ها را بدانیم، کافی ست که دقت کنیم که در Octet دستکاری شده، 2 بیت مختص Host ID می باشد، پس دو را به توان این 2 می رسانیم که می شود : 4 .
پس چهار زیرشبکه خواهیم داشت، که به صورت زیر، در آمده و ترتیب شمارش آنها از خود 32 شروع می شود:

194.167.32.0	til	192.167.32.255	for 255 Host
194.167.33.0	til	192.167.33.255	for 255 Host
194.167.34.0	til	192.167.34.255	for 255 Host
194.167.35.0	til	192.167.35.255	for 255 Host

پس برای نمایش محدوده ی این شبکه بصورت کاملاً خلاصه:

194.167.32.0 - 192.167.35.255

:Example3

می خواهیم آدرس 121.0.0.0/17 را بررسی کنیم.
همانطور که پیداست، در A Class قرار دارد، با یک Prefix Notation یا Net mask غیراستاندارد یا Classless، و با توجه به اینکه Net mask آن از حالت Classfull در B Class بیشتر است، ما با یک حالت Supernetting مواجه هستیم.
پس برای پیدا کردن آدرس Subnet mask آن، باید 17 بیت را برای Net ID نگهداریم:

11111111.11111111.10000000.00000000

که بصورت مقابل می شود: **255.255.128.0**

همانطور که می بینید، یک آدرس در A Class نیز می تواند، آدرس Subnet کاملاً متفاوتی با حالت معمول داشته باشد.
پس بخش های Net ID و Host ID این آدرس را به صورت زیر می توان نشان داد :

121.0.0.0

برای پیدا کردن تعداد Subnet ها کافی ست که دو را به توان تعداد بیت های Host باقیمانده در اکتت دستکاری شده کنیم که می شود: **128**
برای پیدا کردن تعداد Host های قابل آدرس دهی، کافی ست که دو را به توان تمام بیت های مختص Host ID که 15 عدد هستند، کنیم که می شود: **32,766** عدد.
پس برای نمایش محدوده ی این شبکه بصورت کاملاً خلاصه:

121.0.0.0 - 121.0.127.255

128 زیر شبکه را می توان به صورت زیر نشان داد:

121.0.0.0	til	121.0.0.255	for 255 Host
121.0.1.0	til	121.0.1.255	for 255 Host
121.0.2.0	til	121.0.2.255	for 255 Host
…	…	…	…
121.0.127.0	til	121.0.127.255	for 255 Host

:Example4

بررسی کنید که آیا آدرس های IP زیر با Subnet mask های مشخصی که دارند، در شبکه های یکسانی با هم قرار دارند یا خیر؟

1)
192.168.32.20 255.255.255.192
192.168.32.59 255.255.255.192

می توانیم بطور حفظی بیاد آوریم که برای دریافت عدد 192، نیاز به دو بیت اول از Octet مورد نظر داریم، پس تنها شش بیت در Octet آخر این دو IP برای Host ID در نظر گرفته می شوند، و Net Mask برای این IP برابر است با 26 .
پس تعداد Host ID های قابل پشتیبانی می شود «دو به توان شش» یعنی 64.
اما همانطور که می دانیم، هر Octet می تواند عددی بین صفر تا 255 باشد.
پس برای اینکه دو کامپیوتر با سابنت 255.255.255.192، در یک شبکه قرار بگیرند، باید عضو بازه ی 64 تایی یکسانی از آدرس 192.168.32.0 باشند.
اگر 64÷255 را انجام دهیم، می بینیم که می توان 4 بازه داشت.
برای اینکه این محدوده ها را شناسایی کنیم، از صفر شروع می کنیم و هر 64 آدرس را جدا می کنیم.

نکته ریاضیاتی:

فرض کنید بخواهیم از 2 شروع کرده و بشمریم و هر 10 مقدار را جدا کنیم. دو حالت دارد:
اگر بخواهیم بر حسب میزان یا مقدار ریاضیاتی این تفکیک را انجام دهیم:

2 + 10 = 12
13 + 10 = 23
24 + 10 = 34

اگر بخواهیم بر حسب تعداد، این تفکیک را انجام دهیم:

2 + 10 = 11
12 + 10 = 21
22 + 10 = 31

در حقیقت وقتی قصد حساب کردن تعداد، در یک محدوده را داشته باشیم، فقط تعداد آنها مهم می شود که متفاوت از ارزش خود آن عدد می باشد.

یعنی وقتی که دو را با 10 جمع می کنیم و می شود 12، این 12 مجموع مقادیری است که در بازه های این ارقام وجود دارند، اما اگر تعداد را بخواهیم، خود عدد 2 نیز به نوعی دارای ارزش فیزیکی می شود، و هنگام شمارش، از روی خود دو شمرده و جلو می رویم که در پایان، یک عدد کمتر از نتیجه ی ریاضیاتی می شود.

0 + 64 = 63
64 + 64 = 127
128 + 64 = 191
192 + 64 = 255

192.168.32.0	til	192.168.32.63	for 64 Host
192.168.32.64	til	192.168.32.127	for 64 Host
192.168.32.128	til	192.168.32.191	for 64 Host
192.168.32.192	til	192.168.32.255	for 64 Host

پس این دو آدرس، در یک شبکه و در یک زیرشبکه قرار دارند.

2)

192.168.48.32 255.255.255.240

192.168.48.50 255.255.255.240

می توانیم بطور حفظی بیاد آوریم که برای دریافت عدد 240، نیاز به 4 بیت اول از Octet مورد نظر داریم، پس تنها چهار بیت در Octet آخر این دو IP برای Host ID در نظر گرفته می شوند.

پس 2^4 تعداد برای Net ID و همچنین 2^4 تعداد برای Host ID خواهیم داشت، یعنی 16 زیر شبکه و در هریک از آنها 16 آدرس.

192.168.48.0	til	192.168.48.15	for 16 Host
192.168.48.16	til	192.168.48.31	for 16 Host
192.168.48.32	til	192.168.48.47	for 16 Host
192.168.48.48	til	192.168.48.63	for 16 Host
…	…	…	…

پس همانطور که می بینید، این دو آدرس، در یک شبکه قرار ندارند.

:Example5

فرض کنید در یک ساختمان اداری، یک شبکه ی بزرگ، شامل 150 کامپیوتر داریم و می خواهیم آنها را شبکه کنیم.

با توجه به اینکه در Class C تا 254 کامپیوتر را می توان آدرس دهی کرد، و ما فقط 150 کامپیوتر داریم، پس Class C را انتخاب می کنیم.

پس مشخصات شبکه بصورت زیر می شود:

Network address	192.168.0.0
Subnet mask	255.255.255.0

اما نکته اینجاست که این 150 کامپیوتر در سه طبقه ی مختلف پخش هستند، و می خواهیم کامپیوترهای هر طبقه، آدرس یکسان با هم و متفاوت با طبقات دیگر داشته باشند.

پس باید Supernetting انجام دهیم.

با فرض اینکه در هر طبقه حداکثر 50 تا 60 کامپیوتر وجود دارد، باید آدرس دهی را به Subnet هایی که تا 50 یا 60 آدرس را پشتیبانی می کنند، بشکنیم.

پس دو بیت از بیت های Host ID در Subnet mask را به Net ID اضافه می کنیم.

11111111.11111111.11111111.00000000 > 11111111.11111111.11111111.11000000

درنتیجه هر زیرشبکه می تواند حداکثر 64 کامپیوتر را آدرس دهی کند و نه بیشتر.البته اگر آدرس Network و Broadcast را از آن کسر کنیم، برابر با 62 می شود.

اما حال می خواهیم بدانیم چند زیر شبکه یا Subnet می توان تشکیل داد، یا به عبارتی توسط این Supernetting تا چند طبقه را می توان به شبکه اضافه کرد.که جواب می شود :

$$2^{(\text{تعداد بیت های Host که دستکاری شدند})} = 2^2 = 4$$

پس بخش های Net ID و Host ID به شکل زیر می شوند:

192.168.0.0 / 26

پس 4 زیرشبکه می توان داشت :

Subnet 1	00000000 - 00111111	(.0 - .63)
Subnet 2	01000000 - 01111111	(.64 - .127)
Subnet 3	10000000 - 10111111	(.128 - .191)
Subnet 4	11000000 - 11111111	(.192 - .255)

و Subnet Address بصورت زیر می شود:

255.255.255.192

Subnet Dividing :

تا اینجا آموختیم که چطور با یک **IP Address**، یک **Network** را طوری آدرس دهی کنیم که چند **Subnetwork** داشته باشیم.
حال می آموزیم که هر **IP Address** قادر به آدرس دهی چندین **Network** است که هریک دارای چند **Subnetwork** هستند.
ویژگی ها و مزایای این عملیات:

- اعضای هر یک از بخش ها، از طریق **Ping** به اعضای بخش های دیگر دسترسی ندارند.
- **Routing table** ها سبک تر می شوند.
- **Security** و **Management** قوی تر و بهینه تری خواهیم داشت.

Example1:

می خواهیم آدرس **172.28.0.0/18** را بررسی کنیم.
همانطور که پیداست، **IP** در **B Class** تعریف شده است، با یک **Classless Net mask**، **که در حالت Supernetting قرار دارد.**
پس برای پیدا کردن آدرس **Subnet mask** آن، باید **18** بیت را برای **Net ID** نگهداریم:

11111111.11111111.11000000.00000000

که بصورت مقابل می شود: **255.255.192.0**

پس بخش های **Net ID** و **Host ID** این آدرس را به صورت زیر می توان نشان داد :

172.28.0.0

برای پیدا کردن تعداد **Host** های قابل آدرس دهی، کافی ست که دو را به توان تمام بیت های **Host ID** که **14** عدد هستند، کنیم که می شود: **16,384** عدد.
برای پیدا کردن تعداد **Subnet** ها کافی ست که دو را به توان تعداد بیت های **Host** در **octet** دستکاری شده کنیم که می شود: **64**
برای پیدا کردن تعداد **Net** هایی که با این **IP** می توان ساخت، کافی ست دو را به توان تعداد بیت های **Net** در **octet** دستکاری شده کنیم: **4** .
نمایش اولین محدوده ی اولین شبکه ی قابل ساخت توسط این **IP** بصورت کاملاً خلاصه:

172.28.0.0 - 172.28.63.255

4 شبکه را می توان به صورت زیر نشان داد:

Subnet 0	172.28.0.0/18	-	172.28.63.255/18	for 16,384 Host
Subnet 1	172.28.64.0 /18	-	172.28.127.255/18	for 16,384 Host
Subnet 2	172.28.128.0 /18	-	172.28.191.255/18	for 16,384 Host
Subnet 3	172.28.192.0 /18	-	172.28.255.255/18	for 16,384 Host

:Example2

می خواهیم به کمک آدرس **186.128.32.0/19** پانزده **Network** مجزا داشته باشیم.

همانطور که پیداست، **IP** در **B Class** تعریف شده است، با یک **Classless Net mask**، که در حالت **Supernetting** قرار دارد.
ابتدا آدرس **Subnet mask** آن را پیدا می کنیم:

11111111.11111111.11100000.00000000

که بصورت مقابل می شود: **255.255.224.0**

- در حقیقت تعداد کل **Network** هایی که با این **IP** می توان آدرس دهی کرد، می شود: **32**
- در حقیقت آن سه بیت اول، به منظور تقسیم بندی **Network** ها، جدا شده بوده است، برای ایجاد **Subnetwork** از این **Netwok**، باید دوباره به تعداد مورد نیاز، بیت به **NetID** اضافه کنیم: $Log_2 15$ **~ 4**
- پس عدد **4**، می شود تعداد بیت های موردنیاز برای ایجاد پانزده عدد **Subnet**.

11111111.11111111.11100000.00000000

پس آدرس **IP** اصلی شبکه بصورت **186.128.32.0 / 23** و آدرس سابنت به صورت **255.255.254.0** خواهد شد.

تعداد **Network** های قابل پیاده سازی: $2^4 = 16$
تعداد **Subnet** های قابل پیاده سازی در هر **Network** : $2^1 = 2$
تعداد کل **Host** های قابل آدرس دهی در هر **Network** : $2^9 = 512$

Network 0	186.128.32.0 /23 til	186.128.32.255 /23	for 255 Host
	186.128.33.0 /23 til	186.128.33.255 /23	for 255 Host
Network 1	186.128.34.0 /23 til	186.128.34.255 /23	for 255 Host
	186.128.35.0 /23 til	186.128.35.255 /23	for 255 Host
Network 2	186.128.36.0 /23 til	186.128.36.255 /23	for 255 Host
	186.128.37.0 /23 til	186.128.37.255 /23	for 255 Host
Network 3	186.128.38.0 /23 til	186.128.38.255 /23	for 255 Host
	186.128.39.0 /23 til	186.128.39.255 /23	for 255 Host
...			
Network 15	186.128.62.0 /23 til	186.128.62.255 /23	for 255 Host
	186.128.63.0 /23 til	186.128.63.255 /23	for 255 Host

:Example3

می خواهیم به کمک آدرس 183.242.0.0 /16 ، 115 شبکه ی مجزا داشته باشیم.

همانطور که پیداست، IP در B Class تعریف شده است.
پس باید به تعداد شبکه هایی که لازم داریم، بیت به Net ID قرض دهیم، که قاعدتاً چون 115 نزدیک به 128 است، 7 بیت قرض می دهیم:
11111111.11111111.11111110.00000000

که Subnet mask بصورت مقابل می شود: **255.255.254.0**
پس آدرس IP اصلی شبکه بصورت 23 / 183.242.0.0 خواهد شد.

- تعداد کل Host های قابل آدرس دهی در هر Net : $2^9 = 512$
- تعداد Subnet های قابل پیاده سازی در هر Net : $2^1 = 2$
- تعداد Net های قابل پیاده سازی: $2^7 = 128$

Network 0:	183.242.0.0 /23	til	183.242.0.255 /23	for 255 Host
	183.242.1.0 /23	til	183.242.1.255 /23	for 255 Host
…				
Network 127:	183.242.254.0 /23	til	183.242.254.255 /23	for 255 Host
	183.242.255.0 /23	til	183.242.255.255 /23	for 255 Host

:Example4

می خواهیم بدانیم آخرین آدرس Valid موجود، در اولین Subnet توسط آدرس 192.168.131.0 /28 چیست؟

Subnet mask به صورت 11111111.11111111.11111111.11110000 می شود : 255.255.255.240
تعداد کل Host های قابل آدرس دهی در هر Net : $2^4 = 16$
تعداد Subnet های قابل پیاده سازی در هر Net : $2^4 = 16$

192.168.131.0 /28 til 192.168.131.15 /28

پاسخ: 192.168.131.14

:Example5

آدرس BroadCast شبکه ی 10.224.16.0 / 255.255.240.0 را بدست آورید.

Subnet mask به صورت 11111111.11111111.11110000.00000000 می شود.
تعداد کل Host های قابل آدرس دهی در هر Net : $2^{12} = 4096$
تعداد کل Subnet ها در هر Net : $2^4 = 16$

Subnet 0	**10.224.16.0 /20**	**til**	**10.224.16.255 /20**	**for 255 Host**
Subnet 1	**10.224.17.0 /20**	**til**	**10.224.17.255 /20**	**for 255 Host**
Subnet 2	**10.224.18.0 /20**	**til**	**10.224.18.255 /20**	**for 255 Host**
	…			
Subnet 15	**10.224.31.0 /20**	**til**	**10.224.31.255 /20**	**for 255 Host**

:Example6

اولین آدرس Valid در شبکه یا Subnet ای که شامل IP مقابل است، کدام است: **192.168.101.58/29**

به عبارتی می خواهیم بدانیم آدرس بالا، عضو کدام Subnetwork است.

Subnet mask به صورت 11111111.11111111.11111111.11111000 می شود.

روش اول:

تعداد کل Host های قابل آدرس دهی در هر Net : $2^3 = 8$

تعداد کل Subnetwork ها در هر Network : $2^3 = 8$

Subnet 0	192.168.101.0 /29	til	192.168.101.7 /29
Subnet 1	192.168.101.8 /29	til	192.168.101.15 /29
Subnet 2	192.168.101.16 /29	til	192.168.101.23 /29
Subnet 3	192.168.101.24 /29	til	192.168.101.31 /29
Subnet 4	192.168.101.32 /29	til	192.168.101.39 /29
Subnet 5	192.168.101.40 /29	til	192.168.101.47 /29
Subnet 6	192.168.101.48 /29	til	192.168.101.55 /29
Subnet 7	192.168.101.56 /29	til	192.168.101.63 /29 => پاسخ

روش دوم:

دو را به توان تعداد بیت های دست نخورده ی اوکتت آخر مربوط به آدرس Subnet می رسانیم: 2^3 که می شود 8.

عددی که در آخرین اوکتت IP موردنظر است را تقسیم بر 8 می کنیم: 58÷8 که می شود: 7

حال 7 را در 8 ضرب می کنیم: 56

:Example7

شما مدیر IT سازمانی هستید که 3 واحد و حدود 190 کامپیوتر دارد، که در هر واحد حدود 40 کامپیوتر وجود دارد.

شما از رنج 192.168.10.X برای شبکه ی سازمان استفاده کرده اید.

در این حالت تمام کامپیوتر ها با هم Ping شده و ارتباط دارند.

از بالا دستور آمده که هیچ واحدی نباید با واحد دیگر ارتباط داشته باشد.یعنی هر 6 واحد فقط بتوانند با کامپیوتر های واحد خود ارتباط داشته باشند.

به روش های گوناگونی می توان این کار را اجرایی کرد:

- استفاده از Switch های لایه 3
- جداسازی اتصالات شبکه ی هر واحد
- استفاده از رنج های IP گوناگون
- استفاده از Subnetting :

ایده ی اصلی کار، تغییر Subnet mask است، نه تغییر رنج IP.

مشکل اینترنت، Gateway و Active Directory :

اگر کلاینت های شما به اینترنت متصل می شدند و الان هم باید به اینترنت متصل باشند باید به ازای هر رنج، یک Gateway در همان رنج داشته باشید.

:VLSM Example

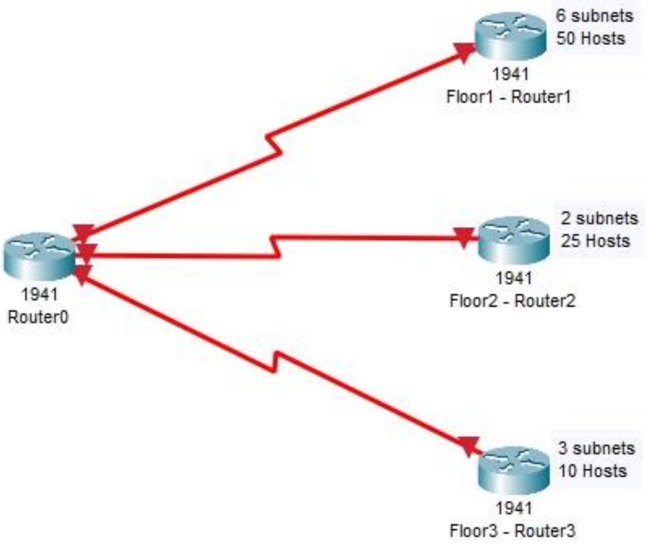
درواقع برخی سایت های VLSM Calculator نیز وجود دارند که این تفکیک و محاسبات Subnet را به سادگی و با چند کلیک انجام می دهند.
تنها کافی ست که آدرس IP موردنظر را مشخص کنید و درج کنید که به چند Subnet نیاز است و چه نام هایی داشته باشند.

فرض کنید که در یک ساختمان بزرگ، سه بخش بزرگ وجود دارد که برای هریک، یک Router تدارک دیده ایم.

- **Router0 مربوط به خود بخش IT شرکت است.**
- **آدرس IP مقابل را برای این شبکه ی بزرگ درنظر گرفته ایم:**

192.168.32.0 /23

- **مطابق شکل زیر، Router های یک تا سه مربوط به این سه بخش سازمان هستند.**
- **همانطور که در کنار هریک از Router ها درج شده است، برای هریک از بخش ها، نیاز به چند Subnet هستیم که هریک باید تعداد موردنظری Client را پشتیبانی کنند.**
- **هریک از Router ها، از سمت خارجی، باید با Router0 که مربوط به بخش IT می باشد، متصل باشند.**



درحقیقت می توانیم این آدرس دهی را به دلخواه از هریک از بخش ها شروع کنیم. پس ما در اینجا از Router1 شروع می کنیم.

:Router1

$Log_2{}^{50} \sim 5.6 = 6$ تعداد بیت های Host

پس آدرس Network و Subnet آن به شکل زیر خواهند بود:

192.168.32.0 /26
255.255.255.192

و دارای شش Subnet خواهیم بود که هریک دارای 64 آدرس Host خواهند بود.

محدوده ی آدرس های این شش Subnet به شرح زیر خواهند بود:

192.168.32.0	til	192.168.32.63
192.168.32.64	til	192.168.32.127
192.168.32.128	til	192.168.32.191
192.168.32.192	til	192.168.32.255
192.168.33.0	til	192.168.33.63
192.168.33.64	til	192.168.33.127

همانطور که می بینیم، اگر تمام آدرس های شبکه ی Subnet مصرف می شوند، به سادگی شروع به مصرف آدرس های شبکه ی بعدی می کنیم.

:Router2

Log$_2$ ^{25} ~ 4.6 = **5** تعداد بیت های Host

پس آدرس **Network** و **Subnet** آن به شکل زیر خواهند بود:

192.168.33.128 /27
255.255.255.224

و می توانیم دارای هشت **Subnet** باشیم، که هریک دارای **32** آدرس **Host** خواهند بود، البته در اینجا تنها به دو **Subnet** نیاز داریم.

پس محدوده ی آدرس های این دو **Subnet** به شرح زیر خواهند بود:

192.168.33.128 til 192.168.33.159
192.168.33.160 til 192.168.33.191

:Router3

Log$_2$ ^{10} ~ 3.6 = **4** تعداد بیت های Host

پس آدرس **Network** و **Subnet** آن به شکل زیر خواهند بود:

192.168.33.192 /28
255.255.255.240

و می توانیم دارای شانزده **Subnet** باشیم، که هریک دارای **16** آدرس **Host** خواهند بود، البته در اینجا تنها به سه **Subnet** نیاز داریم.

پس محدوده ی آدرس های این سه **Subnet** به شرح زیر خواهند بود:

192.168.33.192 til 192.168.33.207
192.168.33.208 til 192.168.33.223
192.168.33.224 til 192.168.33.239

:Router0

درحقیقت، در اینجا هر سه **Router** دیگر را، **Subnet** های **Router0** در نظر می گیریم.

پس به سه **Subnet** نیاز است، که هریک حداکثر دو آدرس **Valid** را پشتیبانی کنند.

چون همیشه دو آدرس اول و آخر، جهت Network و Broadcast مصرف می شوند، مجبوریم مقدار 4 بیت برای Host را مورنظر قرار دهیم.

Log$_2$ ^{4} ~ = 2 تعداد بیت های Host

پس آدرس **Network** و **Subnet** آن به شکل زیر خواهند بود:

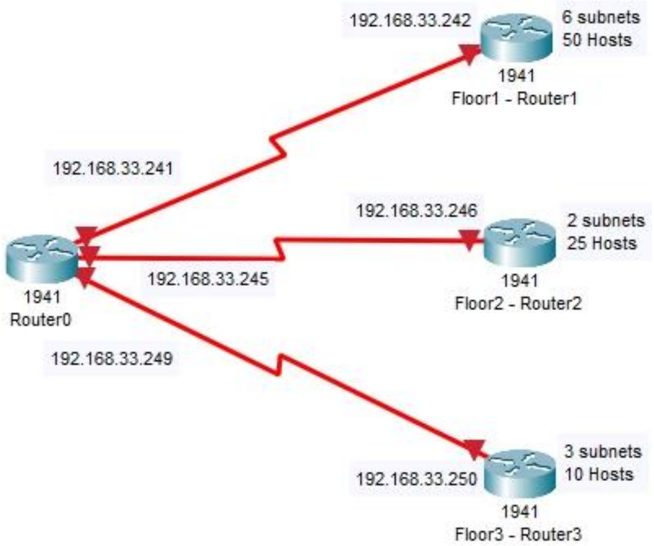
192.168.33.240 /30
255.255.255.252

و می توانیم دارای شانزده **Subnet** باشیم، که هریک دارای **16** آدرس **Host** خواهند بود، البته در اینجا تنها به سه **Subnet** نیاز داریم.

پس محدوده ی آدرس های این سه **Subnet** به شرح زیر خواهند بود:

192.168.33.240 til 192.168.33.243
192.168.33.244 til 192.168.33.247
192.168.33.248 til 192.168.33.251

پس آدرس های **Gateway** خارجی مربوط به **Router** ها به شکل زیر خواهند بود:



PowerShell :

- Shell : به هرمحیطِ دارای Command Line، که در آن بتوان با سیستم عامل ارتباط برقرار کرد، Shell گفته می شود.
- مزیت Shell، قابلیت خودکار سازی وظایف و سرعت عمل در انجام کارهاست.
- PowerShell : یک Shell برای محصولات Microsoft است، که همچنین مشابه یک محیط برنامه نویسی (IDE) جهت Script نویسی نیز می باشد.
- بستر Script نویسی PowerShell، نسخه ی PowerShell ISE (Integrated Scripting Environment) است.
- اولین نسخه PowerShell در نوامبر 2006 برای ویندوز XP و ویندوز Server 2003 منتشر شد.
- این ابزار قدرتمند ، مبنی بر Net Framework. می باشد؛ پس به Class ها و Method های زیادی دسترسی دارد.
- هم می تواند بصورت Local کار کند و هم به صورت Remote.
- دستورات Powershell با دستورات cmd و با دستورات Linux Shell کاملاً متفاوت هستند، اما در محیط Powershell می توان هم از دستورات cmd استفاده کرد و هم از تعداد زیادی از دستورات Linux Shell.
- دستورات پاورشل Command-let یا cmdlet نام دارند.
- می توان هر دستور یا متنی را با ماوس در آن Copy/Paste کرد.
- Tab Completion: دارای قابلیت Command Builder می باشد، یعنی می توان بخشی از دستور را تایپ کرده و کلید Tab را فشرد تا ادامه ی آن به صورت خودکار درج شود.
- PowerShell برای اسم ها، Case Sensitive است، اما برای دستورهای خودش حساس نیست!

معمولاً سه راه برای فراخوانی PowerShell وجود دارد:

- جستجو در منوی Start : با درج powershell
- جستجو در Run : با درج powershell
- درج نام powershell در صفحه ی cmd

سعی کنید همیشه PowerShell را به صورت Run as Administrator اجرا کنید.

می توان برای شناسایی ورژن PowerShell درون آن تایپ کرد:

```
$PSVersionTable
```

ساختار Cmdlet ها به این صورت است که همیشه ابتدا یک فعل می آید، سپس یک خط تیره و سپس یک اسم!

- برای مشاهده ی همه ی دستورهای موجود در PowerShell:

```
Get-Command
```

- برای مشاهده ی همه ی دستورهای موجود که یک فعل یا یک اسم خاص را در بر می گیرند:

```
Get-Command -Verb get
Get-Command -Noun content
```

1. فعل ها مثل: Get، Add، Set، Remove و ....

برای دیدن همه ی فعل های PowerShell از دستور زیر استفاده می کنیم:

```
Get-Verb
```

برای پیدا کردن همه ی فعل هایی که با یک حرف خاص (مثلاً S) شروع می شوند/ یا به S ختم می شوند:

```
Get-Verb -verb s*
Get-Verb -verb *s
```

2. اسم ها مثل: Service، User، Command، Content، Location و ....

نکته: این اسم ها، همیشه به صورت مفرد هستند.

- فرض کنید بخواهیم تمام دستورهایی که در آنها کلمه ی new وجود دارد را ببینیم:

```
Get-Command *new*
```

مثال: تمام دستوراتی که با کلمه ی dns شروع می شوند:

```
Get-Command DNS*
```
یا
```
Get-Command -Name DNS*
```

برای اینکه از خروجی یک دستور، فقط یک سری اطلاعات را فیلتر کرده و مشاهده کنیم، از علامت **Pipe** که بصورت **|** می باشد، استفاده می کنیم. مثلاً برای لیست کردن **Service** های سیستم از دستور زیر استفاده می شود:

```
Get-Service
```

- برای لیست کردن **Service** هایی که در سیستم بصورت **Stop** هستند:

```
Get-Service | Where-Object Status -EQ stopped
```

- برای لیست کردن **Role** هایی که در سیستم نصب هستند:

```
Get-WindowsFeature | Where-Object installed -EQ True
```

در حقیقت، هر ستون در یک لیست، یک **Object** نام دارد.پس وقتی پارامتر شرطیِ **where-object** می آید، به معنی یک شرط برای مقدار یک ستون است؛ که بالافاصله نام آن ستون را پس از شرط درج می کنیم.

EQ- به معنای «برابر است با» می باشد.

- اگر بخواهیم نتیجه را به شکل ستون هایی با فاصله های متناسب نشان دهد، می توانیم از سوییچ **ft** استفاده کنیم، که بعد از آن نام ستونها را یکی یکی درج می کنیم:

```
Get-Service | ft Status,Name,DisplayName
```

- اگر بخواهیم که در نتیجه ی ظاهر شده، نام ستون ها نشان داده نشوند، سوییچ **ft** را به اینصورت وارد می کنیم: `|ft -hide`
- اما اگر بخواهیم فقط خود محتویات مربوط به یک ستون را (مثلاً ستون DisplayName) دریافت کنیم:

```
Get-Service | select DisplayName -ExpandProperty DisplayName
```

در حقیقت محتوایی که به این شکل دریافت می شوند، درون یک آرایه قرار دارند. هر سطر از آن، یک سلول از این آرایه است.

- اگر بخواهیم نتیجه را در یک فایل **Notepad** به نام مثلاً **list** ذخیره کنیم، از سوییچ **Out-File** استفاده می کنیم.

```
Get-Service | Out-File c:\list.txt
```

- اگر بخواهیم نتیجه را بصورت کپی شده داشته باشیم، تا در جایی مثل **Notepad** آنرا **Paste** کنیم:

```
Get-Service | clip
```

- اگر بخواهیم تعداد نتایج را بدست بیاوریم، باید توسط علامت **Pipe** از سوییچ **measure** استفاده کنیم:

```
Get-Service | measure
```

در حقیقت اکثر دستورها در **PowerShell** دارای یک نسخه کوتاه شده هم هستند، که بصورت اختصار از یک دستور هستند، که به آن **Alias** گفته می شود، که شباهت زیادی با دستورات لینوکسو یا با دستورات **CMD** دارند.

برای دیدن همه ی **Alias** ها در **PowerShell**:

```
Get-Alias
```

- می توانیم خودمان بطور دلخواه برای یک دستور، **Alias** تعریف کنیم، مثلا تعیین کلمه ی **serv** برای دستور **Get-Service**:

```
Set-Alias -Name serv -Value Get-Service
```

- برای دریافت راهنمایی درمورد یک دستور کافی ست قبل از درج آن دستور، کلمه ی **man** یا **help** را درج کرد، **Example**:

```
Get-Help Get-Service
 Man Get-Service
```

- و اگر از راهنمایی ها، هنوز درست متوجه یک دستور نشدید، می توانید به شکل زیر، درخواست **Example** هم بدهید:

```
Man Get-service -examples
```

- برای دریافت راهنمایی درمورد یک دستور بطور کامل و واضح در خود سایت **Microsoft** :

```
man Get-Service -Online
```

- این راهنمایی های **PowerShell** را با دستور زیر **Update** می کنیم. معمولاً پس از نصب **Role** ها یا **Feature** ها الزامی است:

```
Update-help
```

گاهی ممکن است این دستور **Update** با شکست مواجه شود، پس از دستور زیر استفاده می کنیم:

```
Update-Help -Verbose -Force -ErrorAction SilentlyContinue
```

وقتی که **help** را برای یک **cmdlet** می زنید، مهم ترین بخش خروجیِ آن، بخش **Syntax** است که همه ی پارامترها و نوع ورودی های آنها را برای آن نشان می دهد.

به مجموعه ی یک **cmdlet** همراه با پارامترهایی که برای آن تعریف می شود، **Syntax** گفته می شود، مثلاً:

```
Get-Service -Name … -ComputerName … -
```

مثلاً:

```
New-ADUser [-Name] <String> [-AccountExpirationDate <DateTime>] [-AccountNotDelegated <Boolean>]
```

- بخش هایی که درون [ ] قرار دارند، یعنی اجباری به درج و تعیین کردن آنها نیست.
- بخش هایی که درون < > قرار دارند، یعنی حتماً باید درج و تعیین شوند.
- همانطور که می بینیم، گاهی می توان از درج نام یک پارامتر صرفنظر کرد، اما از مقدار آن نمی توان!

- توسط دستور زیر، می توانیم خط آدرس کنونی را دقیقاً ببینیم:

```
Get-Location
```

- می توانیم این خط آدرس را توسط ..cd و \cd تغییر دهیم.
- ما می توانیم توسط دستور **dir** و یا **ls** ، محتویات خط آدرسی که در آن هستیم را ببینیم.
- توسط دستور زیر، علاوه بر اینکه می توانیم محتویات خط آدرس جاری را ببینیم، می توانیم با درج سوییچ **-Path** یک آدرس را برای آن تعیین کنیم تا محتویات آن را نیز ببینیم:

```
Get-ChildItem -Path <Address>
```

در پاسخ **dir** یا **Get-ChildItem** ستونی به نام **Mode** قرار داد که در این ستون، یکی یا حتی همه ی حروف زیر، می توانند برای هر سطر روشن باشند که معنی مشخصی خواهند داشت:

d (**Directory**): یعنی این گزینه، یک **Folder** است.

r (**Read**): مجوز خواندن دارد.

w (**Write**): مجوز نوشتن دارد.

- توسط دستور زیر، می توانیم بررسی کنیم که آیا **Folder** یا **File** موردنظر، موجود است یا خیر:

```
Test-Path -Path C:\Folder1
Test-Path -Path C:\Folder1\file.txt
```

:Sort the result

برای اینکه نشان دهیم نتایج به چه شکل تنظیم و ظاهر شوند، همیشه در پایان دستور، ابتدا یک علامت پایپ (**|**) درج می کنیم و سپس از چندین گزینه می توان استفاده کرد، بطورمثال:

- هریک از نتایج را به شکل یک سطر نمایش می دهد که مشخصات آن، در ستون های جداگانه درج خواهند بود. اما نتایج طولانی را به شکل کوتاه شده نشان می دهد.

```
Format-Table
```

- هریک از نتایج را به شکل یک سطر نمایش می دهد که مشخصات آن، در ستون های جداگانه درج خواهند بود. هر ستون را تا جایی که همه ی مقادیر طولانی هم قابل نمایش باشند، پهن می کند.

```
Format-Table -AutoSize
```

- گاهی سطر یا سطرهای نتیجه ی ظاهرشده، آنقدر طولانی است که خود **powerShell** (یا در **EMS**) به جای درج ادامه ی سطر، تنها سه نقطه درج می کند! پس از درج **wrap** در پایان استفاده می کنیم:

```
Format-Table -AutoSize -Wrap
```

- هریک از نتایج را به شکل یک پاراگراف نشان می دهد که مشخصات آن به شکل زیرگزینه در زیر آن درج می شوند:

```
Format-List
```

و یا

```
FL
```

- اگر پس از **FL** از علامت ستاره استفاده کنیم (**| FL ***)، اطلاعات را بصورت مفصل، لیست می کند.

: Repository

تمامی **Cmdlet** های **PowerShell** به شکل طبقه بندی شده، درون مخزن (**Repository**) های مخصوص قرار دارند.
مخزن اصلی و پیشفرض، که همه ی دستورات معمول **PowerShell** درون آن قرار دارند، **PowerShell Gallery** (**PSGallery**) نام دارد.

➢ برای مشاهده ی این مخزن، یا در صورت وجود، مشاهده ی همه ی مخزن ها:

```
Get-PSRepository
```

نکته1: اگر در پاسخ دستور بالا، در ستون **InstallationPolicy** کلمه ی **Untrusted** درج شده بود، دستور زیر را یکبار وارد می کنیم:

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
```

نکته2: اگر در پاسخ این دستور بالا، خط زیر را دریافت کردیم:

WARNING: Unable to find module repositories.

○ ابتدا دستور زیر را وارد کرده و پس از اتمام، یک بار **PowerShell** را بسته و دوباره امتحان می کنیم:

```
Register-PSRepository -Default -Verbose
```

○ اگر هنوز همان خطای **unable to find module** را داد؛ به ترتیب دستورهای زیر را وارد می کنیم:

```
[Net.ServicePointManager]::SecurityProtocol
[Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor [Net.SecurityProtocolType]::Tls12
[Net.ServicePointManager]::SecurityProtocol
Register-PSRepository -Default -Verbose
```

این **Repository** شامل بسته بندی هایی برای دستورات است، که به هریک از آنها **Module** گفته می شود.

➢ برای مشاهده ی تمامی **Module** های موجود:

```
Get-InstalledModule
```

- برای مشاهده ی جزییات و برخی Cmdlet های یک Module :

```
Get-Module -ListAvailable ModuleName
```

مثال:

```
Get-Module -ListAvailable PowerShellGet
```

- برای مشاهده ی همه ی Cmdlet های یک Module:

```
Get-Command -Module PowerShellGet
```

- برای حذف یک Module (مثلاً PowerShell Get):

```
Uninstall-Module -Name PowerShellGet -Force
```

برای استفاده از برخی Service ها، باید ابتدا Module مخصوص به دستورات آن Service را فراخوانی و نصب کرد، به صورت زیر:

```
Install-Module -Name نام سرویس -Repository PSGallery
```

گاهی لازم است که PSGallery را Update کرد. به ترتیب، دستورات زیر را وارد می کنیم:

```
Install-PackageProvider -Name NuGet -Force -Debug -Verbose
Install-Module -Name PowerShellGet -Force -Verbose -Debug
Update-Module -Name PowerShellGet -Force -Verbose -Debug
```

اگر بجای انجام هریک از دستورات نصب و بروزرسانی Module یا Packege با خطایی مشابه با خط زیر مواجه شدیم:

```
PowerShell Gallery is currently unavailable
```

که اولین علت آن، عدم پشتیبانی از TLS ورژن یک می باشد؛ پس باید آنرا تغییر دهیم:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

اگر بازهم نشد:

https://www.powershellgallery.com/packages/PowerShellGet/2.2.5
https://docs.microsoft.com/en-us/powershell/scripting/gallery/how-to/working-with-packages/manual-download?view=powershell-7

: Principles

همانطور که می دانیم برخی از دستورهایی که در **PowerShell** یا حتی در **cmd** می نویسیم، یک سری **Task** ها را انجام می دهند.
(یعنی همیشه تست یا نمایش گزینه ها و مشخصات نیست.)
مثلاً وظیفه ی خاموش کردن یا **Restart** کردن سیستم:

```
shutdown -r -t 0
```

حال اگر بخواهید این وظیفه را به شکل یک آیکونِ همیشه در دسترس که با یک دابل کلیک اجرا شود، در دسترس داشته باشید، کافی ست این دستور را در **Notepad** درج کرده و آنرا با یک **Name** دلخواه و با یکی از دو پسوند زیر ذخیره کنیم (**Type را All Files قرار می دهیم**):

- **PS1.** : چه **Script** درج شده، از دستورات **PowerShell** باشد، و چه از دستورات **cmd** باشد، می تواند با این پسوند ذخیره شود.
- **CMD.** : این پسوند فقط مخصوص **Script** های **cmd** است و دستورات **PowerShell** را نمی فهمد!

نکته: برای اجرای **Script** هایی (فایل PS1.) که یک کاری را انجام می دهند، باید کلیک راست کرده و **Run with PowerShell** را بزنیم.

نکته: برای اجرای **Script** هایی (فایل PS1.) که یک نتیجه را اعلام می کنند، با دسترسی مدیریتی، وارد **PowerShell** شده و در صورتی که **Command line** در مسیر زیر قرار داشته باشد:

C:\WINDOWS>

دستور زیر را وارد می کنیم:

system32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Bypass -file "C:\ABC.ps1" DomainName\UserName

نکته: **Username** ای که در این دستور وارد می کنیم، نیازی نیست که حتماً دسترسی **admin** داشته باشد.

: Delete Windows Apps

```
Get-AppxPackage | Select Name, PackageFullName
```

برای حذف یکجا و همزمان تعدادی از App های غیرضروری Windows می توانیم دستور زیر را کاملاً درون یک Notepad درج کرده و با پسوند ps1. ذخیره کرده و فایل ذخیره شده را در هر سیستم دلخواهی اجرا کنیم:

```
Get-AppxPackage -Name * windowscommunicationsapps* | Remove-AppxPackage
Get-AppxPackage -Name *yourphone* | Remove-AppxPackage
Get-AppxPackage -Name *storepurchaseapp* | Remove-AppxPackage
Get-AppxPackage -Name *MusicParadise* | Remove-AppxPackage
Get-AppxPackage -Name *ZuneVideo* | Remove-AppxPackage
Get-AppxPackage -Name * PeopleExperienceHost* | Remove-AppxPackage
Get-AppxPackage -Name *MixedReality* | Remove-AppxPackage
Get-AppxPackage -Name * 3DBuilder* | Remove-AppxPackage
Get-AppxPackage -Name * Xbox.TCUI* | Remove-AppxPackage
Get-AppxPackage -Name *BingNews* | Remove-AppxPackage
Get-AppxPackage -Name *BingFinance* | Remove-AppxPackage
Get-AppxPackage -Name * BingSports* | Remove-AppxPackage
Get-AppxPackage -Name * XboxGameCallableUI* | Remove-AppxPackage
Get-AppxPackage -Name *XboxSpeechToTextOverlay* | Remove-AppxPackage
Get-AppxPackage -Name *Microsoft.Wallet* | Remove-AppxPackage
Get-AppxPackage *bingnews* | Remove-AppxPackage
Get-AppxPackage *bingweather* | Remove-AppxPackage
Get-AppxPackage *candycrush* | Remove-AppxPackage
Get-AppxPackage *maps* | Remove-AppxPackage
Get-AppxPackage *messaging* | Remove-AppxPackage
Get-AppxPackage *officehub* | Remove-AppxPackage
Get-AppxPackage *skypeapp* | Remove-AppxPackage
Get-AppxPackage *solitaire* | Remove-AppxPackage
Get-AppxPackage *twitter* | Remove-AppxPackage
Get-AppxPackage *windowsphone* | Remove-AppxPackage
Get-AppxPackage *zunemusic* | Remove-AppxPackage
Get-AppxPackage *XBOXzunevideo* | Remove-AppxPackage
```

در اداره جات:

```
Get-AppxPackage *connectivitystore* | Remove-AppxPackage
```

:Net Framework.

برای اینکه ببینیم چه نسخه هایی از این افزونه، بر روی سیستم نصب است، ابتدا نیاز به نصب ابزار مربوط به آن داریم:

```
Install-Module -Name DotNetVersionLister -Scope CurrentUser -Force
```

اگر نصب آن با خطا روبرو شد، ابتدا پکیج NuGet را به ترتیب توسط دستورات زیر نصب می کنیم:

```
[Net.ServicePointManager]::SecurityProtocol
[Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor
[Net.SecurityProtocolType]::Tls12
[Net.ServicePointManager]::SecurityProtocol
Register-PSRepository -Default -Verbose

Set-PSRepository -Name PSGallery -InstallationPolicy Trusted

Install-PackageProvider -Name NuGet -Force -Debug -Verbose
Install-Module -Name PowerShellGet -Force -Verbose -Debug
Update-Module -Name PowerShellGet -Force -Verbose -Debug
```

سپس توسط دستور زیر لیست آن را دریافت می کنیم:

```
Get-STDotNetVersion
```

:Points

- برای نشان دادن یا پنهان کردن Script Pane، از **CTRL+R** استفاده می کنیم.
- وقتی از دستوراتی که یک سری فرآیندها را طی می کنند، استفاده می کنیم،(مثل Import و ...) می توانیم از سوییچ **-verbose** در پایان syntax استفاده کنیم، تا مراحلی که انجام می دهد و همچنین Cmdlet هایی که ایجاد می شوند را (به شکل فیروزه ای رنگ) نمایش دهد.
- فرض کنید باید یک دستور خیلی طولانی بنویسیم که برای درج و دیدنِ انتهای خط دستوری، نیاز باشد که scroll bar را مدام به سمت راست و چپ حرکت دهیم! برای اینکه بتوانیم ادامه ی یک دستور را در خط بعد پیش ببریم، بدون اینکه خللی در اجرای آن ایجاد شود، یک فاصله و سپس علامت ` را درج می کنیم و ادامه ی دستور را در خط بعد درج می کنیم.
- وقتی از دستورات کنترل User های Active Directory استفاده می کنیم، گاهی در یک دستور برای درج نام User، از پارامتر **-user** استفاده می کنیم و گاهی از پارامتر **-Identity** .
  - وقتی که می خواهیم توسط یک دستور، در تنظیمات یک User جستجو کنیم و اطلاعاتی کسب کنیم، از Identity- استفاده می کنیم.
  - وقتی که می خواهیم در تنظیمات تمامی User ها، مشخصات یک User خاص را جستجو کنیم، از User- استفاده می کنیم.

Windows Task Schedular:

توسط این کنسول، می توان یک سری فرآیند ها را تنظیم و زمان بندی کرد که به طور خودکار، در زمان های مورد نظر، اجرا شوند.
این فرآیندها می توانند:

- **توسط ابزارهای Windows انجام بگیرند،**
- **توسط نرم افزارهای نصب شده روی Windows انجام بگیرند،**
- **توسط یک سری دستورات به هم پیوسته، که به آن Script گفته می شود، انجام بگیرند.**

این Script ها را هم می توان توسط Command prompt تنظیم کرد، و هم می توان توسط PowerShell نوشت.

- **آن فرآیند، می تواند ارسال ایمیل، خاموش کردن کامپیوتر، حذف کردن فایل‌های درون یک فولدر موردنظر و ... باشد.**
- **به هریک از این فرآیند هایی که در این Console تنظیم می شوند تا بطورخودکار اجرا شوند، Task گفته می شود.**

بطورپیشفرض، چند Task در این کنسول تعریف شده اند، مثل update های ویندوز که هر از گاهی بطور خودکار اجرا می شوند.

ایجاد یک Task:

ابتدا بر روی سیستم یک Service Account ایجاد می کنیم. (فرقی نمی کند اگر یک Account معمولی local باشد با دسترسی admin)
نکته: این Service Account، می تواند یک Account معمولی در AD باشد که گزینه ی Password never expire را برای آن فعال کرده باشیم و دسترسی های مدیریتی لازم را داشته باشد، مثل:

- دسترسی به سیستم مدیریت نرم افزار شبکه
- دسترسی کامل به Server های شبکه
- دسترسی مدیریتی بر روی سیستم های Client های شبکه
- عضویت در گروه Domain Admin

وارد منوی Action شده و گزینه ی Create Task را می زنیم.
در تب General:

- **یک نام و یک توضیح مختصر برای این Task درج می کنیم.**
- **در قسمت Author می بینیم که چه کسی آن را ایجاد خواهد کرد.**
- **جهت اجرا کردن هریک Task، لازم است که از طریق سطح دسترسی یک Account انجام شود، پس در قسمت Security Options، توسط Change User or Group، حساب Service Account را انتخاب می کنیم.**

نکته: ساده ترین انتخاب، انتخاب حساب System است، که همه ی دسترسی های موردنیاز تحت سیستم را دارا خواهد بود. اما:

- درصورت کار با این کنسول روی یک سیستم غیر Domain ای، حسابی که در اینجا وارد می کنیم، باید حتمن عضو گروه Administrators باشد.
- درصورت کار با این کنسول روی یک Server، حسابی که در اینجا وارد می کنیم، باید حتمن عضو گروه Domain Admins باشد.

- **بطورمعمول، گزینه ی Run whether user is logged on or not را انتخاب می کنیم، چرا که نیازی به Login کردن روی سیستم نباشد. پس Task، تنها نیاز خواهد داشت که کامپیوتر روشن بوده و دست کم، به صفحه ی آبی ورود به سیستم رسیده باشد، که به این حالت At Startup گفته می شود.**

نکته: این ابزار، جهت اجرا کردن Script هایی که نیاز به ارتباط با نرم افزارهای دیگر (نرم افزارهای غیر ماکروسافتی) ندارند، مشکلی ندارد.
اما جهت اجرای **Script هایی که نیاز به ارتباط با نرم افزار یا ابزارهای غیر مایکروسافتی** (مثل Firefox) دارند، لازم است که در این تب، گزینه ی Run only when user is logged on را فعال کنیم.

نکته: در کامپیوترهایی که عضو Domain نیستند، تنها با یکی از حساب های local یا Administrator یا System می توان Task ها را اجرا کرد.
به شکل زیر:
نام یوزرنیم \ نام کامپیوتر

به این معنی که در سیستم های workgroup، Task ها، به شکل **user specific** کار می کنند.

- ✓ گزینه ی Run with highest privileges را هم فعال می کنیم.
- ✓ در مقابل Configure for، نسخه ی فعلی ویندوز را انتخاب می کنیم.

اما بر روی سیستم Server:

- ✓ می توان از یک Service Account جهت اجرای Task ها استفاده کرد.
- ✓ با هربار وارد شدن به تنظیمات Task، درصورت ایجاد هرگونه تغییر، لازم است که رمزعبور آن Account را وارد کنیم.
- ✓ در صورت امکان، گزینه ی Do not store password را نیز فعال می کنیم.

- در تب Trigger، با کلیک بر روی Triggers با کلیک روی New می توان یک زمانبندی جهت اجرای Task را ایجاد کرد.
- گزینه ی Begin the task، بطور معمول روی On a Schedule قرار دارد که می توان زمانبندی مشخصی را تعریف کرد؛ اما گزینه های دیگر آن نیز کاربردی هستند:
- **On a schedule**: در یک بازه زمانی معین
  - **At log on**: پس از ورود به سیستم
  - **At startup**: پس از بالا آمدن سیستم، فارغ از اینکه ورود انجام شود یا نشود.
  - **On idle**: وقتی که سیستم بیکار می شود.
  - **On an event**: زمانی که یک اتفاق در ویندوز رخ می دهد.
  - **At task creation/modification**: هرزمان که یک Task را ایجاد یا تصحیح می کنیم.
  - **On connection to user session**: زمانی که یک User خاص، به سیستم ورود می کند.
  - **On disconnect from user session**: زمانی که خروج از سیستم (sign out) رخ می دهد.
  - **On workstation lock**: زمانی که سیستم lock می شود.
  - **On workstation unlock**: زمانی که سیستم از lock خارج می شود.

- **در تب Actions، تعیین می کنیم که چه اتفاقی بیفتد.**
- **پس New Action را زده و Start a program را انتخاب کرده و برای** Program/Script **آدرس فایل اجرایی برنامه ی موردنظر، مثلاً PowerShell یا Command Prompt در سیستم را درج می کنیم.**

"C:\WINDOWS\system32\cmd.exe"
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

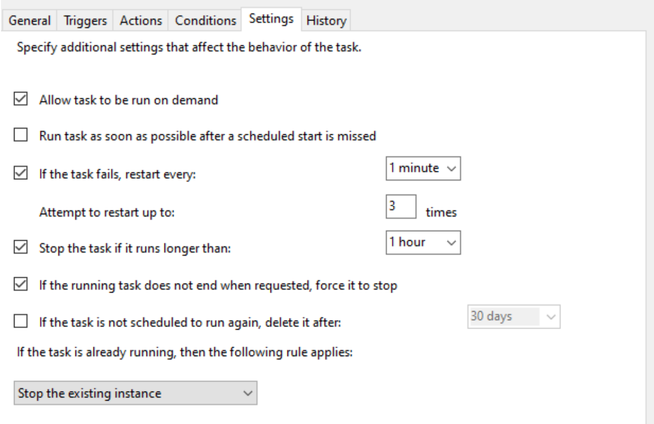
نکته: به علامت های " " که آدرس برنامه ی موردنظر در میان آنها قرار می گیرند، دقت کنید که حتمن باید این علامت استفاده شود.

درحقیقت می توان چندین Action برای یک Task تعریف کرد.

بطور پیشفرض، تاریخچه ی اجرای Task ها، خاموش است، پس از آنجایی که تاریخ اجراهای Task ها اهمیت زیادی دارد، در کادر سمت چپ، یکبار بر روی Task Schedular Library کلیک و سپس کلیک راست کرده و Enable All Tasks History را می زنیم.

- گزارش های اجرا و اتمام هر Task، در کادر پایین و در تب History اش درج می شوند.
- به ازای هربار اجرای موفقیت آمیز یک Task، شش پیام اطلاعاتی (Information) ثبت می شود.
- برای بدست آوردن مدت زمان کامل اجرای یک Task، کافی ست، زمان ایجاد اولین پیام را با زمان ایجاد آخرین پیام هریک اجرای آن، مقایسه کنیم.
- در صورت بستن پنجره ی کنسول Task Schedular، هیچ خللی در روند اجرای Task ها پیش نخواهد آمد.

- **در دو تب Conditions و Settings گزینه ها را بر اساس نیاز، می توانیم تغییر دهیم. به عنوان مثال، می توان:**
  - در تب Conditions ، همه ی گزینه ها را خاموش کرد.
  - تب Settings را به شکل زیر تنظیم کرد:



مثال:

برنامه ریزی و اجرای زمانبندی شده ی یک PowerShell Script:

از طریق خود کنسول Task Schedular انجام می دهیم:

- **در ابتدا Script ای که توسط PowerShell نوشته شده است را با پسوند PS1. ذخیره می کنیم.**
- **وارد Task Schedular شده و از کادر سمت چپ، وارد یکی از پوشه های موردنظر می شویم، و یا در همان پوشه/مسیر ش Task Schedular Library کلیک راست کرده و Create Task را می زنیم.**
- **تنظیمات همه ی تب ها را انجام داده و در پایان وارد تب Action شده، New Action را زده و Start a program را می زنیم:**
  - **برای Program/Script ، نام فایل اجرایی PowerShell را درج می کنیم:**

powershell.exe

یا اینکه مسیر کامل آن را:

“C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe”

- **برای Add arguments، آدرس Script ای که نوشته و ذخیره کرده ایم را به صورت زیر درج می کنیم:**

-File "C:/MyScripts/SCRIPT.ps1"

البته می توان یک سوییچ ExecutionPolicy را نیز جهت اجرای مطمین تر فایل، در پشت Argument اصلی درج کرد:

-ExecutionPolicy Bypass -File "C:/MyScripts/SCRIPT.ps1"

نکته: به علامت های “ ” که آدرس Script در میان آنها قرار می گیرند، دقت کنید که حتمن باید این علامت استفاده شود.

نکات:

- برای مشاهده ی Task هایی که ایجاد کرده ایم، کافی ست در کادر سمت چپ کنسول، فقط پوشه ی Task Scheduler Library را انتخاب کنیم.
- می توان به جهت نظم در کار، از طریق منوی Action و گزینه ی New Folder پوشه یا پوشه هایی را ایجاد کرد و Task های موردنظر را در آنها قرار داد.
- در Script ای که در فایل PowerShell اجرایی، درج می کنیم، بهتر است که در انتهای دستورهایی که نیاز به تاییدیه دارند، از پارامترهای زیر (بسته به نوع آن دستور) استفاده کرد، که پس از اجرای Task ها، نیازی به ارتباط و تاییدیه گرفتن از کاربر نداشته باشند:

```
-Force
-Confirm:$true
-ForceDownload
-ForceInstall
-noninteractive
```

- درحقیقت وقتی در یک سیستم WorkGroup، یک Task، یک فایل PowerShell را جهت اجرای یک دستور باز می کند، آن را بدون دسترسی Admin باز می کند، پس گاهی لازم است که یک Script یا یک Command، با دسترسی مدیریتی اجرا شود.
پس می توانیم برای نوار Add Arguments، مقدار زیر را درج کنیم:

- **اجرای خودکار یک Command با دسترسی Admin:**

```
Start-Process powershell.exe -Verb RunAs { Invoke-Command -ScriptBlock { powershell.exe -noninteractive -Command {XXX -Force}}}
```

- **اجرای خودکار یک Script با دسترسی Admin:**

```
Start-Process powershell.exe -Verb RunAs {Invoke-Command -ScriptBlock {powershell.exe -noninteractive -File "C:/MyScripts/SCRIPT.ps1" -force -Confirm:$true }}
```

- **اجرای خودکار ابتدا یک Command و سپس یک Script، با دسترسی Admin:**

```
Start-Process powershell.exe -Verb RunAs { Invoke-Command -ScriptBlock { powershell.exe -noninteractive -Command {XXX -Force} -File "C:/MyScripts/SCRIPT.ps1" -force -Confirm:$true}}
```

Scheduled task samples :

مثال: فرض کنید بخواهیم در یک زمان خاص، یک وبسایت باز شود.
وارد ویزارد ایجاد یک **Task** شده و در تب **Action** گزینه ی **Start a program** را زده و:

روش اول:

- توسط **Browse** ، فایل اجراییِ یک برنامه ی مرورگر را انتخاب می کنیم. مثلاً برای **Firefox**:

"C:\Program Files\Mozilla Firefox\firefox.exe"

- در کادر **Add arguments**:
  - آدرس سایت موردنظر را درج می کنیم، مثلاً : http://www.imdb.com

روش دوم:

- برای نوار Program/Script توسط Browse ، فایل اجراییِ خود برنامه ی **PowerShell** را انتخاب می کنیم:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

- ابتدا یک فایل **PowerShell** حاوی دستور زیر را ذخیره می کنیم (مثلن با نام SCRIPT):

```
Start-Process "https://www.imdb.com"
```

- در کادر **Add arguments**، دستور زیر را وارد می کنیم:

-ExecutionPolicy bypass -File "C:\Users\Payam.Avarwand\MyScripts\SCRIPT.ps1"

مثال:

- **فرض کنید بخواهیم کامپیوتر را در یک زمان خاص خاموش کنیم.**
  - در کنسول **Task Scheduler** وارد ویزارد ایجاد یک **Task** شده و در تب **Action** گزینه ی **Start a program** را زده و توسط **Browse** به آدرس C:\Windows\System32 رفته و فایل shutdown.exe را انتخاب می کنیم.

- **جهت افزودن یا تغییر تنظیمات Task ها، کافی ست که پس از ایجاد یک Task، روی آن دابل کلیک کرده و تغییرات موردنظر را اعمال کرد.**

گاهی پس از اعمال تغییرات و کلیک بر روی OK با خطایی مشابه missing the required arguments needed to execute the task مواجه می شویم، که باید در تب General گزینه ی Change User or Group را زده و User مدیریتی را انتخاب کرد و سپس سعی در ذخیره ی تغییرات کرد.

مثال: فرض کنید که بخواهیم محتویات پوشه ی **T1** در درایو **C**، هر یک هفته یکبار، حذف شوند.

- ابتدا **Notepad** را باز کرده و متن زیر را در آن کپی می کنیم:

forfiles /p "C:\Users\NAME\Downloads" /s /m *.* /c "cmd /c Del @path" /d -7

- اما مسیری که در کد بالا درج شده را به مسیر پوشه ی خودمان در سیستم تغییر می دهیم.
- عدد ۷ به معنای تعداد روزهایی است که این فرآیند تکرار خواهد شد.

نکته: باید دقت کرد که چهار علامت " که در کد وجود دارد، درست درج شده باشند، وگرنه این کد عمل نمی کند.

- حالا به **File** و سپس **Save As** رفته و این فایل ایجاد شده را، به یک نام دلخواه و با پسوند **.bat** نامگذاری می کنیم.
- برای اطمینان از صحت عملکرد این کد، یکبار آن را اجرا و تست می کنیم.

- **حال در کنسول Task Scheduler وارد ویزارد ایجاد یک Task شده و در تب Action گزینه ی Start a program را زده و توسط Browse آن فایل bat. را وارد می کنیم و تمام!**

مثال: **فرض کنید بخواهیم کامپیوتر را در یک زمان خاص، به حالت sleep وادار کنیم، کاملاً مشابه با مثال قبل عمل می کنیم، اما با کد زیر:**

Rundll32.exe Powrprof.dll,SetSuspendState Sleep

:Create a Task Shortcut

فرض کنید بخواهیم از Task ای که ایجاد کرده ایم، یک Shortcut در Desktop ایجاد کنیم که در مواقع موردنیاز، بدون نیاز به وارد شدن به کنسول Task Schedular، فوری آن را اجرا کنیم.

پس بطورمثال در Desktop کلیک راست کرده و New و Shortcut را می زنیم، و در نوار مربوط به Browse یکی از عبارت های زیر را درج کرده و Next:

schtasks /run /tn "NAMEofTheTASK"
C:\Windows\System32\schtasks.exe /run /tn "NAMEofTheTASK"

نکته: اگر Task موردنظر، درون یک Folder غیر از Folder اصلی برنامه باشد، نیاز است که مکان آن را بطورکامل وارد کنیم، مثلاً:

schtasks /run /tn "\myTasks\NAMEofTheTASK"

در تب Finish، یک نام دلخواه درج کرده و تمام!

نکته: برای اجرای موفقیت آمیز Shortcut دستورهایی که نیاز به حق دسترسی Admin دارند، کافی ست آن Shortcut را با دسترسی Admin باز کنیم.

:Task Scheduler over PowerShell

❖ جهت مشاهده ی Task های موجود:

```
Get-ScheduledTask -TaskPath \XXX\
```

❖ جهت ایجاد یک Task:

```
$scheduledTime = New-ScheduledTaskTrigger -Daily -At 03:24:00
$Action = New-ScheduledTaskAction -Execute
"C:\Windows\System32\WindowsPowerShell\v1.0\PowerShell.exe" -Argument '-file "C:/MyScripts/S1.ps1"'
$UserAccount = "PC01\payam"
$Principal = New-ScheduledTaskPrincipal -UserId $UserAccount -LogonType ServiceAccount -
RunLevel Highest
$Settings = New-ScheduledTaskSettingsSet -ExecutionTimeLimit (New-TimeSpan -Hours 1)

Register-ScheduledTask -TaskName ""\myTasks\TESTTask" -Trigger $scheduledTime -Action $Action
-Principal $Principal -Settings $Settings
```

نکته: پس از اجرای این اسکریپت، یکبار لازم است که چک کنیم که Run whether user is logged on or not غیرفعال باشد.

❖ جهت حذف یک Task:

```
Unregister-ScheduledTask -TaskName "\myTasks\TASKNAME" -Confirm:$true
```

❖ جهت فعال یا غیرفعال کردن یک Task:

```
Disable-ScheduledTask -TaskName "\myTasks\TASKNAME"
Enable-ScheduledTask -TaskName "\myTasks\TASKNAME"
```

: Text

1. در PowerShell اگر یک عدد را درج و اینتر کنیم، نمایش داده می شود.
اما برای برای حروف و متن ها، باید آنها را درون " " و یا ' ' قرار دهیم.
حال اگر بخواهیم چند عدد یا متن را همزمان وارد کنیم، کافیست آنها را درج اما با کاما از هم جدا کنیم.

2. برای بررسی اولین کارکتر یا کاراکترهای یک متن، از سوییچ **match** با علامت **^** استفاده می کنیم.
Case Sensitive نیست.
پاسخ آن یا **true** و یا **False** خواهد بود.

```
'Heyy how are You?' -match '^h'
```

3. برای بررسی آخرین کارکتر یا کاراکترهای یک متن، از سوییچ **match** با علامت **$** استفاده می کنیم.

```
'Heyy how are You' -match 'you$'
```

اگر آخرین کاراکتر، یک علامت خاص مثل : و یا ؟ باشد، باید تمام محتوای مورد بررسی را درون **[]** قرار دهیم.

```
'Heyy how are You?' -match '[you?]$'
```

4. برای اینکه متنی را علامتگذاری کنیم، می توانیم برای پشتِ آن، یک رنگ انتخاب کنیم و یا رنگ خود متن را تغییر دهیم.

```
Write-Host "hey how are you" -ForegroundColor Blue -BackgroundColor Yellow
```

5. برای اینکه ببینیم کلمه یا جمله ای، درون یک متن است یا خیر:

```
'Heyy how are You?' -match 'how'
```

پاسخ آن یا **true** خواهد بود، در صورتی که کلمه ی درون متن **heyy** می باشد! اما اگر دقیقاً بخواهیم وجود کلمه ی **heyy** را بررسی کنیم:

```
'Heyy how are You?' -match ' hey '
```

نکته: اگر در متن مورد بررسی، علامت ' را داشته باشیم، برای جداسازی خود متن ها، از "" استفاده می کنیم:

```
"Heyy what's your name?" -match "hey"
```

6. برای اینکه ببینیم در متن موردنظر، کلمه ای وجود دارد که با حرف یا حروف خاصی شروع می شود، از علامت **\w** که به معنی «هر یک کلمه» می باشد، استفاده می کنیم:

```
'Heyy how are You?' -match 'yo\w'
```

نکته: تمام این **match** هایی که بصورت **boolean** پاسخ داده می شوند (**False/True**) در یک متغیر پیشفرض به نام **matches** ذخیره می شوند و به صورت پیشفرض، فقط آخرین کلمه ای که **match** بوده است را نمایش می دهد. برای فراخوانی این متغیر:

```
$Matches
```

در حقیقت همه ی **match** ها را توسط اندیس گذاری، درون خود ذخیره می کند، که آخرین **match**، دارای اندیس صفر می باشد.
می توان یک سری عملیات بر روی هریک از **match** ها انجام داد یا اطلاعاتی از آنها دریافت کرد.
مثلاً برای دریافت طول یکی از **match** ها :

```
$Matches[0].Length
```

7. اگر چند متن داشته باشیم که بخواهیم وجود یک کلمه را در آنها بررسی کنیم، آنها را درون یک **Array** قرار می دهیم و در پاسخ، متنی که شامل آن کلمه است را نشان خواهد داد:

```
("[what's your name?]","what is that?.") -match ' is '
```

Variable :

1. برای تعریف یک متغیر و مقداردهی به آن، از علامت $ استفاده می شود، بصورت زیر:

$Name = value

مثلاً ایجاد یک متغیر از نوع String و یک متغیر از نوع integer :

```
$Esm = “ali”
$number = 20
```

نکته: نام متغیر از نوع String، نمی تواند فقط یک حرف باشد!

2. برای فراخوانی مقدار یک متغیر، کافی ست علامت $ و سپس نام آن را درج و اینتر کنیم:

```
$Esm
```

3. هر متغیر می تواند چندین value دریافت کند، فقط باید آنها را با کاما از هم جدا کرد:

```
$a2 = "ali","reza","omid"
```

زبان Scripting در پاورشل، Method های زیادی را پشتیبانی می کند که این Method ها برای متغیرهای مختلف، متفاوت می باشند.

4. برای مشاهده ی Method هایی که بر روی یک متغیر قابل اعمال هستند:

```
$Ebarat | Get-Member
```

5. برای اطلاع از نوع یک متغیر، از پسوند ()GetType. استفاده می کنیم، که در پاسخ، در ستون Name، نوع آن درج خواهد شد. مثال:

```
$Esm.GetType()
```

6. ما می توانیم از یک متغیر، در متغیرهای دیگر هم استفاده کنیم. مثال:

```
$Ebarat= "Man $Esm hastam, ba Shomareye $number."
```

Man ali hastam, ba Shomareye 20.

7. برای دریافت اطلاعات از کاربر، از سوییچ Read-Host استفاده می کنیم، مثال:

```
$Question= Read-Host "what is your Number?"
```

در جواب آن، می توانیم هرچیزی درج کنیم!

8. اما برای اینکه فقط ورودی های عددی کاربر را بپذیرد، می توانیم تعیین کنیم که نوع داده ای که در متغیر Question می تواند وارد شود، فقط از نوع عددی است:

```
[int]$Question= Read-Host "what is your Number?"
```

9. برای بررسی اینکه درون محتویات متغیر Ebarat، کلمه ی man وجود دارد یا نه:

```
$Ebarat.Contains("man")
```

که پاسخ می دهد: False، چرا که درون متغیر Ebarat کلمه ی «من» با M بزرگ درج شده است، در غیراینصورت می شد: True

10. برای بررسی اینکه آیا مقدار یک متغیر عددی، برابر با عددی دلخواه است یا نه:

```
$number.Equals(20)
```

11. برای تبدیل یا جایگزینی یک مقدار، با یک مقدار دیگر، در متغیر String ، مثال:

```
$jomle = "i have a book, you have a book"
$jomle.Replace("a ","the ")
```

12. می توانیم Name سیستم جاری را درون یک متغیر قرار دهیم، مثلاً :

```
$d1=(hostname)
```

13. می توانیم یک IP و یا نام یک User را درون متغیر قرار دهیم، مثلاً :

```
$ip = "192.168.1.10"
$user = "Administrator"
```

14. برای تبدیل محتویات یک متغیر متنی بطورکامل به حروف بزرگ یا به حروف کوچک:

```
$T1 = "HeeeeeeeeY"
$T1.ToUpper()
$T1.ToLower()
```

15. برای بررسی اینکه کلمه ای موردنظر، درون یک متن موجود در یک متغیر است یا خیر:

```
$T1="Hey How Are You?"
$T1.Contains("Are")
```

پاسخ True را می دهد. اما باید بدانیم که این دستورات، به حروف کوچک و بزرگ حساس هستند!

نکته: یک ترفند برای اینکه از سد **Case Sensitivity** مربوط به **Contains** کرد و درهرصورت، همه ی مواردی که شامل کلمه ی موردنظر هستند را نشان دهد، یا درهرصورت، پاسخ **True** شود، این است که ابتدا فیلد موردنظر را **capitalize** کنیم (به حروف بزرگ تبدیل کردن) و سپس برای دستور **Contain**، عبارت موردنظر را به صورت کاملاً **Capitalized** وارد کنیم:

```
$T1="hey, how Are You?"
$T1.ToUpper().Contains("YOU")
```

16. می توانیم یک عبارت یا کلمه را درون یک متغیر، یکبار با یک کلمه ی دیگر جایگزین کنیم، اما همچنان مقدار آن متغیر بی تغییر می ماند:

```
$T1="hey, how Are You?"
$T1.Replace("You","we")
```

اما اگر بخواهیم که بطوردائمی این جایگزینی انجام بگیرد:

```
$T1="hey, how Are You?"
$T1 = $T1.Replace("You","we")
```

17. فرض کنید یک متن داشته باشیم، و بخواهیم بخشی از ابتدا و انتهای آن را حذف کنیم:

```
$p="0123456789"
$p.Substring(3,5)
```

پس از سومین کاراکتر متن شروع می کند، و به اندازه ی تا پنج کاراکتر بعدی را نگه می دارد:

```
345678
```

همانطور که می بینید، هریک از کاراکترهای یک متن، دارای یک اندیس هستند که از سمت چپ و از صفر شروع می شود و به آن **Index** گفته می شود.

18. برای پیدا کردن **Index** مربوط به یکی از کاراکترهای متن:

```
$t1="https://mail.yahoo.com/"
$t1.IndexOf("y")
```

19. اگر بخواهیم، بخشی از متن را تا یک بخش مشخص، داشته باشیم:

```
$t1="https://mail.yahoo.com/"
$t2=$t1.Substring(0,$t1.IndexOf("y"))
```

اما فقط تا قبل از **y** را ذخیره می کند، پس به تعداد حروف **yahoo**، به آن یک مقدار را اضافه می کنیم:

```
$t1="https://mail.yahoo.com/"
$t2=$t1.Substring(0,$t1.IndexOf("y")+5)
```

```
https://mail.yahoo
```

20. اگر بخواهیم بخشی از ابتدا و بخشی از انتهای یک متن را حذف کرده و در یک متغیر جدید قرار دهیم:

```
$t1="https://mail.yahoo.com/"
$t2=$t1.TrimStart("https://mail.")
$t2=$t2.TrimEnd("/")
```

:Use of variables

- جهت پیدا کردن **Hostname** سیستم جاری:

```
$H = (HOSTNAME)
$H
```

و یا

```
$Comp = Get-Childitem env:computername
$Comp
```

:Time

دریافت تاریخ و ساعت این لحظه:

```
Get-Date
```

دریافت تاریخ و ساعت 30 روز پیش، در همین لحظه:

```
(Get-Date).adddays(-30)
```

وقتی دستور Get-Date را وارد می کنیم، نتیجه را به شکل پیشفرض نمایش می دهد.

پس ما همچنین می توانیم قالب تاریخ و ساعت نتیجه را نیز خودمان تعیین کنیم، و حتی یک متن به آن اضافه کنیم. مثال:

```
Get-Date -Format 'dd-MM-yyyy "at" hh:mm:ss'
```

در اینجا، کلمه ی at را به دلخواه اضافه کرده ایم، که می توان آن را حذف کرد؛ همچنین برای سال، می توان تنها دو حرف y درج کرد.

نکته: مهم است که:

- حروف ماه، به شکل دو M بزرگ،
- حروف روز، دو d کوچک،
- حروف سال، چهار y کوچک،
- و هر بخش از حروف ساعت، دو حرف کوچک،

باشند.

: Operators

1. همه ی عملگرهایی که در همه ی زبانهای برنامه نویسی استفاده می شوند، در PS هم معتبر هستند:

Arithmetic Operators : مثلاً می توان هریک از عبارات زیر را درج و اینتر کرد تا نتیجه را دید:

```
5+3
5-3
5/3
5*3
5%3
```

2. در مورد اعداد و درج آنها نیز قوانینی وجود دارد، مثلاً:

```
12+"2"  :14
"12"+2  :122

2*"45"  : 90
"2"*45  : 222222222222222222222222222222222222222222222
```

3. می توان **عملگرهای وظیفه ای (-= و *= و /= و %= و ...)** را بر روی متغیرهای عددی اعمال کرد:

```
$a=20
$a+=10
```

نکته : **a+=1** را می توان به صورت **a++** هم درج کرد.

حال اگر مقدار متغیر **a** را بازخوانی کنیم، برابر با **30** شده است.

4. **عملگرهای رابطه ای (relational) با نام Comparison یا مقایسه ای شناخته می شوند** که برای اعداد، به صورت زیرمی باشند:

-eq	==	Equal to
-ne	!=	Not Equal to
-gt	>	Greater than
-ge	>=	Greater than or Equal to
-lt	<	Less than
-le	<=	Less than or Equal to

مثال:

```
5 -eq 3
5 -ne 3
```

پاسخ این دو عبارت، به ترتیب **False** و **True** می شود.

5. **عملگرهای مقایسه ای برای String** ها:

-like	برای بررسی اینکه دو عبارت کاملاً یکسان هستند یا نه!
-notlike	برای بررسی اینکه دو عبارت، بطورکامل یکسان نباشند!
-match	وجود شباهت بین دو عبارت را بررسی می کند.
-notmatch	عدم وجود شباهت بین دو عبارت را بررسی می کند.

مثال:

```
"Alireza" -like "Ali"
"Alireza" -notlike "Ali"
"Ali" -like "Ali"
"Alirez" -match "Ali"
"Alireza" -notmatch "omid"
```

پاسخ این عبارات، به ترتیب می شود: **False** و **True** و **True** و **True** و **True**

فرض کنید می خواهیم بررسی کنیم که عبارتی که داریم، با **ali** شروع می شود یا خیر:

```
"alireza" -like "ali*"
```

که پاسخ **True** می شود.

6. **عملگرهای مقایسه ی جمعی یا Collection Comparison** هم نوعی از مقایسه را انجام می دهند:

-contains	برای بررسی یکسان بودن حداقل یکی از چند عبارات با تک عبارت مقصد.
-notcontains	برای بررسی یکسان نبودن حتی یکی از چند عبارات با تک عبارت مقصد.
-in	برای بررسی یکسان بودن یک عبارت، با حداقل یکی از چند عبارات مقصد
-notin	برای بررسی یکسان نبودن یک عبارت، حتی با یکی از چند عبارات مقصد

مثال:

```
"ali","reza" -contains "ali"
"ali","reza" -notcontains "ali"
"ali" -in "ali","reza"
"omid" -notin "ali","reza"""
```

پاسخ این عبارت به ترتیب می شود: True و False و True و True

7. **برای اینکه نتیجه ی یک دستور را (حتی اگر Error باشد) در یک فایل txt ذخیره شود، از علامت > و برای افزودن نتایج جدیدتر به همان فایل txt ، از علامت >> استفاده می شود. مثال:**

هریک از دستورهای زیر را به ترتیب وارد می کنیم:

```
Get-Service -Name *dns* >d.txt
Get-Service -Name *dhcp* >>d.txt
```

حال اگر در Run، درج کنیم: d.txt ، می بینیم که نتیجه ی هر دو دستور وجود دارد.

8. **عملگرهای منطقی یا Logical (-not و ! و -and و -or) هم به شکل زیر قابل استفاده هستند:**

```
$a1="a1"
$a2="a2"
$a1 -and $a2 -contains "a1"
$a1 -or $a2 -contains "a1"
```

پاسخ ها به ترتیب، False و True خواهد بود.

در دستور اول می گوییم، دستور And بین a1 و a2 چه می شود، وقتی که متغیر a1 دارای مقدار a1 باشد؟

در دستور دوم می گوییم، دستور Or بین a1 و a2 چه می شود، وقتی که متغیر a1 دارای مقدار a1 باشد؟

مثلاً می خواهیم دستور موجودیت یک فایل یا پوشه را برعکس دریافت کنیم:

```
-not (Test-Path -path C:\New Folder)
```

به این معنی می شود که اگر پوشه ی New Folder در این آدرس بود، بگو False!

: Array

آرایه، یک ساختارِ یک سطری است، که می تواند تعدادی ستون داشته باشد.
هر آرایه را درون یک متغیر ایجاد می کنیم.

0 Or -3	1 Or -2	2 Or -1

آرایه ای به نام A1 ایجاد کرده و نوع آنرا نیز بررسی می کنیم:

```
$a1 = New-Object System.Collections.ArrayList
$a1.GetType()
```

اما این آرایه هنوز هیچ عضوی ندارد، پس یک سری دستورها هم بر روی آن قابل اعمال نیستند، حتی نمی توان با متد **Get-Member**، متُدهایی که بر روی آن قابل اعمال هستند را دید.
پس برای آن عضو تعریف می کنیم:
اما قبل از آن باید بدانیم که هریک از اعضای آرایه، دارای یک اندیس یا **Index** هستند.
به عبارتی، هریک از خانه های آرایه، دارای یک شماره ی شناسایی هستند، که این **Index** از صفر شروع می شود. مثلاً :

پس از ایجاد مقدار هر سلول، شماره ی **Index** را نیز نشان می دهد.

مثلاً برای ایجاد آرایه ی :

How	Are	You	Are	You	Ok

```
$a1.Add("How")
$a1.Add("Are")
$a1.Add("You")
$a1.Add("Are")
$a1.Add("You")
$a1.Add("Ok")
```

توسط دستورات زیر:
ابتدا یکبار محتویات آرایه را می بینیم.
و بعد تعیین می کنیم که محتویات سلول شماره ی **1**، حذف شود،
و توسط دستور سوم، اولین سلولی که دارای عبارت **You** می باشد را پاک می شود،
و توسط دستور چهارم، شماره ی جدید اندیس سلولی که دارای **Ok** است را مشاهده می کنیم.

```
$a1
$a1.RemoveAt(1)
$a1.Remove("You")
$a1.IndexOf("ok")
```

برای استخراج کردن یا به عبارتی خارج کردن محتویات یک سلول از آرایه، باید آن سلول را توسط اندیسش صدا زده و درون یک متغیر جدید بریزیم:

```
$N1 = $a1[0]
$N2 = $a1[1]
```

نکته: فرض کنید بخواهیم محتوای یکی از سلول های آرایه را با اندیس آن صدا زده و آن را همراه با یک متن نمایش دهیم. پس اندیس را درون پرانتز قرار می دهیم و پس از پرانتز از علامت + برای پیوستن متن به محتوای سلول آرایه استفاده می کنیم.
مثلاً در سلول چهارم آرایه ی **N1** درج شده است: Picture_08_10

```
$Test = ($N1[4])+"_2020"
```

درنتیجه مقدار `$Test` می شود: **Picture_08_10_2020**

فرض کنید آدرس **Distinguished Name** مربوط به چند **Group** در **Active Directory** را به صورت زیر در اختیار داریم:

"CN=SEC-Ticket-User,OU=Ticket,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Ticket-IT,OU=Ticket,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Ticket-Helpdesk,OU=Ticket,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Wiki-Users,OU=Wiki,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Wiki-ITSUP-RW,OU=Wiki,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=EX-SEC-Wiki-ITDOC-RW,OU=Wiki,OU=Security,OU=Global,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=EX-SEC-Ticket-IT,OU=Ticket,OU=Security,OU=Global,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=NIX1_VPN_User,OU=Groups,OU=NIX1,OU=Ausland_RLS,OU=Users,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=EX-SEC-Ticket-User,OU=Ticket,OU=Security,OU=Global,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=RO-Alle-Intern,OU=Rollen,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=Dom?nen-Benutzer,CN=Users,DC=berlin,DC=rolex,DC=net"

می خواهیم محتویات متنی این خطوط را به صورت کامل بررسی کنیم، پس سعی می کنیم که همه ی آنها را به صورت یکجا، درون یک متغیر ذخیره کنیم، با توجه به اینکه هریک از سطرها درون " " قرار دارند، پس این لیست را به صورت یک آرایه ی یک بعدی، درون یک متغیر ذخیره می کنیم.

```
$d1 = {"CN=SEC-Ticket-User,OU=Ticket,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Ticket-IT,OU=Ticket,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Ticket-Helpdesk,OU=Ticket,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Wiki-Users,OU=Wiki,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=SEC-Wiki-ITSUP-RW,OU=Wiki,OU=Security,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=EX-SEC-Wiki-ITDOC-RW,OU=Wiki,OU=Security,OU=Global,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=EX-SEC-Ticket-IT,OU=Ticket,OU=Security,OU=Global,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=NIX1_VPN_User,OU=Groups,OU=NIX1,OU=Ausland_RLS,OU=Users,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=EX-SEC-Ticket-User,OU=Ticket,OU=Security,OU=Global,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=RO-Alle-Intern,OU=Rollen,OU=Universal,OU=Groups,OU=RLS,DC=berlin,DC=rolex,DC=net"
"CN=Dom?nen-Benutzer,CN=Users,DC=berlin,DC=rolex,DC=net"}
```

حال کافی ست که متغیر d1 را، به صورت معمولی فراخوانی کنیم، تا محتویات آن را ببینیم.

برای فراخوانی سطر به سطر محتوای متغیر d1 کافی ست برای فراخوانی آن، یک اندیس درج کنیم.

: Hashtable

مثل Array درون یک متغیر ایجاد می شود، اما ساختار آن، برعکس Array است!
چون یک ساختار دو ستونی است، که می تواند به تعداد دلخواه، ردیف داشته باشد.
ستون اول، Name و ستون دوم، Value (مقدار) نام دارد.
در حقیقت مقدار ستون Name، معرف برای هریک از ردیف هاست که به آن Key هم گفته می شود و نمی تواند تکراری باشد.
مثلاً برای ایجاد جدول زیر:

Esm	Omid
sen	20

```
$tab=@{"esm"="omid";"sen"="20"}
```

البته اجباری نیست که برای تعریف Hashtable فوراً مقدار برای آن تعریف کنیم، می توان فقط آن را تعریف کرد:

```
$tab=@{}
```

حال برای اضافه و یا حذف کردن یک ردیف در این Hashtable :

```
$tab.Add("kar","class")
$tab.Remove("kar")
```

برای دریافت مقادیر Key و یا مقادیر Value از یک Hashtable:

```
$tab.Keys
$tab.Values
```

اما فرض کنید که مقدار یک Key را داشته باشیم (مثلاً Sen)، و مقدار Value آن را بخواهیم:

```
$tab."sen"
```

برای بررسی وجود یک مقدار خاص، در میان Value های جدول(مثلاً 20):

```
$tab.ContainsValue("20")
```

برای بررسی وجود یک Key Name خاص، در میان Name های جدول(مثلاً sen):

`$a1.Contains("sen")` و یا `$ar.ContainsKey("sen")`

Selections :

اصولاً علامت | به جهت شرط گذاری یا جداکردن بخشی از نتیجه ی دستور پشت سرش است.
مثلاً می دانیم که دستور **Get-Proccess**، پردازش های در حال اجرا را نشان می دهد که شامل چند ستون است.
می خواهیم فقط یکی از ستون های آن را ببینیم، مثلاً فقط **ProccessName** :

```
Get-Process | select -Property ProcessName
```

در اینجا **Property** برای مشخص کردن نام ستون است.

- حال می خواهیم مشخص کنیم، از مقادیر موجود برای این ستون، فقط آنهایی را نشان بده که با کلمه ی **win** شروع می شوند:

```
Get-Process | select -Property ProcessName | where {$_.ProcessName -like "win*"}
Get-Service | Where-Object{$_.DisplayName.Contains("Windows")}
```

ProcessName.$_ به معنی «هریک از سطرهایی که ستون **ProccessName** آنها» می باشد.

- ما می توانیم نتیج یک جستجو را، درون یک **HashTable** هم قرار دهیم، که به جای **Pipe** ، فقط یک کاما می گذاریم:

```
Get-ChildItem | select -Property Name, @{Name="Tarikh"; Expression={Get-Date}}
```

- چون قصد لیست کردن مقادیر ستون **Name** را داریم، پس اولین سطر **HashTable** برابر می شود با **Name** و مقدار آن، برابر می شود با **Expression** که به معنای محتویات دریافتی برای **Name** می باشد.

- برای اینکه برای هریک از مقادیر دریافتی، تاریخ آن هم درج شود، برای ستون زیر **Tarikh**، دستور دریافت تاریخ را وارد می کنیم.

- توسط دستور **sort**، می توانیم نتایج یک دستور را به ترتیب الفبا مشاهده کنیم، مثال:

```
Get-ChildItem | sort
```

:Script tricks

- ❖ برای یافتن تعداد نتایج یا تعداد **Object** هایی که در پاسخ یک دستور وجود دارند، در پایان آن، Measure-Object | را درج می کنیم.
- ❖ برای اینکه پس از اجرای یک دستور، سیستم بطورخودکار، **Restart** شود، در پایانِ آن، **-restart** را درج می کنیم.
- ❖ جهت مشاهده ی فقط نام **OU** هایی که در یک مسیر در **Active Directory** قرار دارند:

```
Get-ADOrganizationalUnit -Filter * -SearchBase $DistinguishedName -SearchScope OneLevel | select Name
```

- ❖ گاهی میان دو دستور در یک **Script**، لازم است که یک درنگی وجود داشته باشد، مثلن جهت اینکه از تکمیل فرآیند قبلی مطمین باشیم و سپس دستور بعدی اجرا شود.

پس می توان به شکل زیر، مدت زمانی را صبر کرد، تا پس از آن، دستورات بعدی اجرا شوند:

```
Start-Sleep -Seconds 5
```

- ❖ گاهی لازم است که پاسخ دستورات را درون یک فایل ذخیره کنیم، و سپس آن فایل را به مکانی دیگر کپی یا به هرشکلی ارسال کنیم، طوری که نسخه ی ابتدایی حذف شود.

```
Remove-Item -Path “C:\TEST.xlsx"
```

- ❖ برای تنظیم خروجی های یک دستور، بر اساس یکی از **Field** های آن، می توان در انتها، یک **Pipe** درج و از دستور زیر استفاده کرد:

```
| Sort-Object -Property SamAccountName
```

- ❖ برای پیدا کردن فقط فایل هایی که یک کلمه یا عبارت خاص در یکی از مشخصه های آنهاست (مثلن در Name آنها)؛ پس از درج دستور اصلی، یک **Pipe** درج کرده و از دستور زیر استفاده می کنیم:

```
| Where-Object {$_.Name -Like "*testword*"}
```

- ❖ برای پیدا کردن همه ی فایل ها، به جز آنهایی که یک کلمه یا عبارت خاص در نام آنهاست؛ پس از درج دستور اصلی، یک **Pipe** درج کرده و از دستور زیر استفاده می کنیم:

```
| Where-Object {$_.Name -notLike "*testword*"}
```

نکته: X.$_ به این معنا می باشد: «هر سطری که ستونِ X مربوط به آن»

```
Get-ChildItem | Where-Object {$_.Name.Contains("&")}
```

نکته: $_ به این معنا می باشد: « برای هر سطر یا برای هر ردیف»

نکته: در حقیقت دستورهای toUpper و Contains و replace و ... نمی توانند بطورمستقیم بر روی نام فایل ها اعمال شوند، بلکه باید ابتدا به نام فایل ها اشاره کرد، سپس اعمال کرد!

:Rename the Files

- می خواهیم دقیقاً علامت **&** که در نام همه ی پوشه ها یا فایل های موجود وجود دارد، تبدیل به **and** بشود:

```
Get-ChildItem | Where-Object {$_.Name.Contains("&")} | ForEach-Object
{Rename-Item $_ -NewName $_.Name.Replace("&","and")}
```

- می خواهیم علامت **&** به هرشکلی که در نام همه ی پوشه ها یا فایل های موجود وجود دارد، تبدیل به **and** بشود:

```
Get-ChildItem | Where-Object -Property Name -Like -Value "*&*" | ForEach-Object
{Rename-Item $_ -NewName $_.Name.Replace("&","and")}
```

File :

برای ایجاد و یا حذف یک فایل:

```
New-Item -Name pop.txt -Path F:\
New-Item -Name pop.avi -Path D:\

Remove-Item -Name pop.txt -Path F:\
```

حال اگر این فایل متنی، دارای محتویاتی باشد، برای مشاهده ی آن:

```
Get-Content C:\pop.txt
```

برای تغییر کامل محتویات یک فایل متنی:

```
Set-Content -Path G:\texts\12.txt 'Hey, How R U?'
```

برای افزودن محتویات، به یک فایل متنی:

```
Add-Content -Path G:\texts\12.txt 'What,R U doing?'
```

می توانیم محتویات فایل متنی را درون یک متغیر ذخیره کنیم:

```
$a1 = Get-Content -Path C:\pop.txt
```

برای ایجاد یک فایل **txt** با محتویات :

```
'Hey How Are You? > c:\df.txt
```

برای ایجاد یک فایل **Html** توسط **PowerShell** ، کافی ست کدهای مربوطه را درون "" قرار دهیم:

```
"<h1>Hi From $(hostname) </h1>" > C:\inetpub\wwwroot\example.htm
```

نکته: قبل از `(hostname)` ، علامت **$** قرار دادیم که از کدهای **HTML** متمایز شناخته شود.

برای ایجاد یا حذف یک پوشه:

```
New-Item -Name Folder2 -ItemType Directory
```

اگر سوییچ **ItemType** را درج نکنیم، بطور پیشفرض، آن را **File** در نظر می گیرد.

```
Remove-Item folder2
```

برای حذف همه فایل های با فرمت **txt** که قدیمی تر از **20** ثانیه پیش هستند. البته می توان متد آن را به دقیقه و ماه و ... هم تغییر داد.

```
Get-ChildItem -Path C:\Users\admavar\Desktop\*.txt -Recurse |
Where-Object {$_.LastWriteTime -lt (Get-Date).AddSeconds(-20)}| Remove-Item -Force
```

برای باز کردن هرگونه فایلی:

```
Invoke-Item -Path F:\10.mp4
```

برای ذخیره کردن نتیجه ی یک دستور در یک فایل:

```
Get-ADUser -Identity Payam1 | Out-File -FilePath d:\info.txt
```

البته می توان از سوییچ زیر جهت جلوگیری از **overwrriten** شدن فایل موردنظر استفاده کرد:

```
-NoClobber
```

برای کپی کردن فایل:

مثلاً فایلی از درایو **C** به درایو **E** :

```
Copy-Item -Path 'C:\MyFile.txt' -Destination e:\
```

برای اضافه کردن مقدار خروجی یک دستور، به یک فایل که از قبل دارای محتویات است، بدون اینکه آن محتویات قبلی، حذف شوند:

```
Add-Content -Path "C:\MyFile.txt" -Value (Get-AdUser -Filter *)
```

- توسط دستور بالا، خروجی دستور **Get-AdUser** که برای پارامتر **–Value** درج شده است، به آدرس **Path** اضافه خواهد شد.
- البته می توان این دستور را در انتهای یک دستور کامل، و پس از درج یک | اضافه کرد، که نیازی به پارامتر **–Value** نخواهد داشت.

نکته: در صورت استفاده از Add-Content دیگر نمی توانیم از پارامتر format-Table | استفاده کنیم، چرا که محتویات خروجیِ آن، برای Add-Content قابل درک نخواهند بود.

: CSV Files

می توان از فایل های Excel، توسط گزینه ی Save as به سادگی یک نسخه یcsv. تهیه کرد، مگر اینکه داده های موجود در فایل Excel، تا حد زیادی درهم و پیچیده باشند.

برای اینکه در فایل های csv. مشخص کنیم که دو عبارت متنی در کنار هم، باید در دو سلول مجزا ذخیره باشند، دو روش وجود دارد:

- از روی کیبورد، توسط دکمه ی Tab یک فاصله درج کنیم.
- یک علامت **,** میان آن دو عبارت درج کنیم. (در این حالت، لازم است ابتدا آن فایل متنی اولیه را با فرمت csv. ذخیره و توسط Excel باز کنیم.)

فرض کنید، یک شبکه ی بزرگ داریم و قصد داریم، یک لیست از تمام پرسنلی که دارای یک حساب کاربری فعال در شبکه هستند، در Excel تهیه کنیم که شامل نام و نام خانوادگی و نام شهر و عنوان شغلی هریک از آنها باشد، و ترتیب این لیست، بر اساس شهر آنها باشد.

1. **ابتدا، توسط Script زیر، لیست را در یک فایل notepad ذخیره می کنیم:**

```
$ADD = "OU=Users,OU=RLS,DC=berlin,DC=Network,DC=com"

$Users = Get-ADUser -Filter 'enabled -eq "true"' -SearchBase $ADD -Properties  name, GivenName,
surname, title, city, samaccountname | Select name, GivenName, surname, title, mail, city |
Where-Object {$_.Name -notlike "*test*"} | Sort-Object -Property city

foreach ($u1 in $Users) {
         $UFirstName = $u1.GivenName
         $utitle = $u1.title
         $off = $u1.city
         $ULastName = $u1.surname
  "$UFirstName,$ULastName,$utitle,$off" | Add-Content -Path "Z:\Personal.txt"
}
```

2. **حال این فایل متنی را باز کرده و وارد منوی File و گزینه ی Save as شده و در نوار انتخاب نام فایل مقصد، نوع را از txt. به csv. تغییر داده و نوار Type را بر روی All files تنظیم کرده و ذخیره می کنیم.**
3. **حال که فایلcsv به دست آمده است، آن را با Excel باز می کنیم.**
4. **می بینیم که تک تک سطرها، تنها در ستون اول قرار دارند! پس ستون اول را بطورکامل انتخاب کرده و وارد منوی <u>Data</u> شده و توسط گزینه ی <u>Text to Columns</u> و انتخاب <u>Delimited</u>، کلیه ی ستون ها را با تنظیم علامت Comma به عنوان علامت تفکیک، ایجاد می کنیم.**

   پس در پایان، علامت کاما بطورخودکار حذف خواهد شد.

: Excel files

با توجه به اینکه فایل های اکسل، یک قالب خاص خود را دارند، پیشنهاد می شود که تا جای ممکن، به جای فایل های اکسل، از فایل های با فرمت csv. استفاده شود. (comma-separated values)

- **برای استفاده کار با فایل های Excel در PowerShell، ابتدا لازم است که ماژول مربوط به دستورات آن را نصب کنیم:**

```
Install-Module ImportExcel -Scope CurrentUser
```

- برای مشاهده ی دستورهای مربوط به ماژول Excel می توان از دستور زیر کمک گرفت:

```
Get-Command -Module ImportExcel
```

درحقیقت به دو روش می توان خروجی یک دستور یا Script در PowerShell را، درون یک فایل Excel ذخیره کرد:

1. ذخیره و بازیابی محتویات کلی فایل های Excel توسط PowerShell .

- **در انتهای آن از دستور Export-Excel همراه با درج یک مسیر ذخیره سازی درج می کنیم. مثال:**

```
Get-Command -Module ImportExcel | select Name, CommandType | Export-Excel D:\Comm.xlsx
```

با وارد کردن این دستور:

- **یک فایل Excel و در درون آن، اولین صفحه یا Sheet را ایجاد کرده و پاسخ را در آن ثبت می کند.**
- **اگر آن فایل Excel از قبل موجود بوده باشد، پاسخ دستور جاری، در اولین Sheet و بر روی اطلاعاتی که بوده است، درج** (overwrite) **می شود!**
- **پس اگر در انتهای دستور، یک نام Sheet جدید را تعیین کنیم، یک Sheet با آن نام ایجاد و پاسخ دستور جاری، در آن ثبت می شود.**

```
... | Export-Excel D:\Comm.xlsx -WorksheetName "TEST1"
```

- **فرض کنید یک گزارش حاصل از یک دستور را در یک فایل Excel ذخیره کرده ایم، و لازم است که هر چندوقت یکبار، نتیجه ی جدید آن دستور، در همان فایل Excel و در همان sheet اضافه شود، بدون اینکه به محتویات گزارش قبلی خدشه و تغییری وارد شود.**
  پس کافی ست به انتهای دستور Export-Excel یک سوییچ Append هم اضافه کنیم. مثال:

```
... | Export-Excel D:\Comm.xlsx -WorksheetName "TEST1" -Append
```

نکته: اگر محتویات جدید، دارای ستون های متفاوت از محتویات قبلی باشند، اطلاعات ستون های پاسخ دستور جدید، اضافه نمی شوند!
اما همیشه یک گزارش با ستون های ثابت، به فایل Excel اضافه می شود، پس مشکلی وجود نخواهد داشت.

- **برای فراخوانی محتویات یک صفحه از یک فایل Excel، در PowerShell ، از دستور Import به شکل زیر استفاده می کنیم:**

```
Import-Excel -Path "F:\Test.xlsx" -WorksheetName “TEST1”
```

نکته: اگر نام Sheet را درج نکنیم، به شکل پیشفرض، فقط محتویات اولین Sheet را نمایش می دهد.

- **اگر یک فایل Excel دارای Sheet های زیاد باشد، و ما نام دقیق Sheet موردنظر را ندانیم، به شکل زیر، ابتدا Sheet های آن فایل Excel را لیست می کنیم:**

```
Get-ExcelSheetInfo -Path "F:\Test.xlsx"
```

نکته: اگر تعداد و نام ستون ها، در همه ی Sheet ها، یکسان باشند، به سادگی و توسط Script زیر می توان محتویات همه ی Sheet ها را یکجا فراخوانی کرد:

```
$ADD = "F:\File.xlsx“
$Info = Get-ExcelSheetInfo -Path $ADD
        foreach($sheet in $Info){
        $SheetName = $sheet.Name
        Import-Excel -Path $ADD -WorksheetName $SheetName
        }
```

2. ایجاد یک فایل Excel و اجرا کردن یک سری دستور و ذخیره ی خروجی ها، با یک نظم موردنظر، در تک تک سلول ها.

ساختار لایه های یک فایل Excel جهت ارایه ی اطلاعات، دارای چهار لایه ی تو در تو می باشد:

- **Application Layer: این لایه، بیرونی ترین لایه است که با اجرای نرم افزار Excel، فعال می شود.**

مشابه یک قفسه کتاب است، که جهت دسترسی صحیح و سالم به کتاب ها، ضروری است، و یک عدد از آن کافی و ضروری است.

- **WorkBook Layer: هرگاه که یک فایل Excel را توسط نرم افزار Excel باز می کنیم، درحقیقت، در حال مشاهده ی و کار با یک لایه ی Workbook هستیم. بطور همزمان می توان، چندین Workbook را باز نمود.**

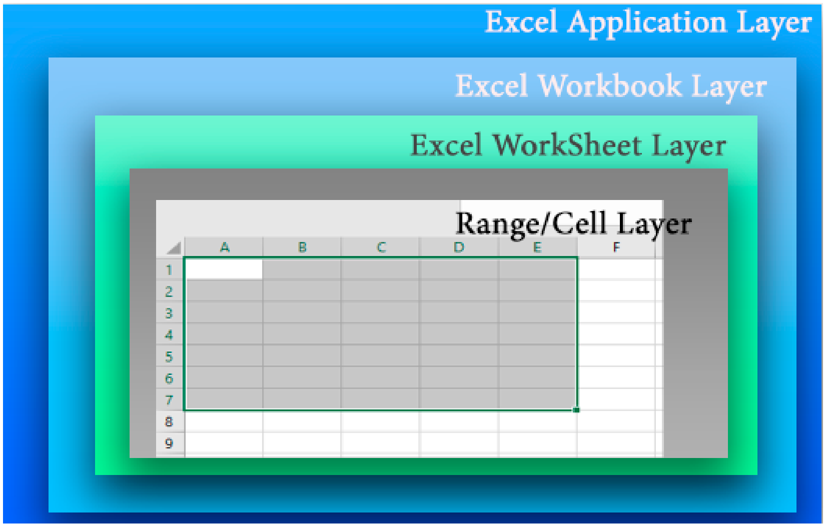
هر Workbook layer، به شکل یک فایل مجزا و با قالب xlsx. ذخیره می شود.

مشابه یک کتاب است، و می توان چندین عدد از آن را ایجاد کرد.

- **WorkSheet Layer: هر لایه ی WorkBook، می تواند شامل چندین، صفحه، با ظاهر و قالب بندی های متفاوت باشند، که به هریک از این صفحات، WorkSheet گفته می شود.**

مشابه یک صفحه از یک کتاب است، که محتوای اصلی، در آن قرار دارد؛ و می توان چندین عدد از آن را ایجاد کرد.

- **Range Layer: کوچکترین و داخلی ترین لایه ی فایل های Excel، یک Cell یا سلول می باشد، که می توان اطلاعات را به شکل مدیریت شده درون هریک از آنها یا محدوده ای شامل چندین عدد از آنها، ذخیره کرد.**



پس جهت ایجاد یک فایل Excel و اجرای یک سری فرآیند و ذخیره ی نتیجه ی آنها درون آن فایل:

- **در ابتدا، با ایجاد یک Object از نوع COM، لایه ی Application مربوط به نرم افزار Excel را فرا می خوانیم، که به شکل نامحسوس و در پشت پرده ی سیستم، روشن خواهد شد؛ و این فراخوانی را درون یک متغیر ذخیره می کنیم:**

```
$Excel_Obj = New-Object -ComObject Excel.Application
```

  - درحقیقت، جهت اطمینان از فراخوانی صحیح این لایه، می توان یکبار نرم افزار Excel را توسط دستور زیر، اجرا کرد:

```
$Excel_Obj.visible = $True
```

  - جهت مشاهده ی همه ی مشخصات این Excel Object، می توان دستور زیر را اجرا کرد:

```
$Excel_Obj | fl
```

- **توسط دستور زیر، یک WorkBook ایجاد کرده و درون متغیر $Workbook ذخیره اش می کنیم:**

```
$Workbook = $excel_Obj.Workbooks.Add()
```

- **توسط دستور زیر، یک WorkSheet ایجاد کرده و درون متغیر $Sheet ذخیره اش می کنیم:**

```
$Sheet= $workbook.Worksheets.Item(1)
```

  - می توانیم نام Sheet را خودمان به شکل زیر، تعیین کنیم:

```
$Sheet.Name = "AB-List"
```

  - سپس توسط دستور زیر، می توان Sheet های موجود در WorkBook مان را لیست کرده و جای آنها را مشاهده کرد:

```
$workbook.Sheets| fl Name, index
```

- **توسط دستور زیر، می توان عبارت First Name را در سلولی که در ردیف یک و ستون دو قرار دارد، درج کنیم:**

```
$Sheet.Cells.Item(1,2) = "First name"
```

  - به همین شکل و با استفاده از متغیرها و دستورهای دیگر، به سادگی می توان اطلاعات را در سلول های فایل Excel ذخیره کرد.
  - در مثال زیر می بینیم که به جای عدد سطر یا ستون و به جای مقدار موردنظر نیز، می توان از یک متغیر استفاده کرد:

```
$Name = 'Payam'
$i1 = 6
$Sheet.Cells.Item($i1,2) = $Name
```

در پایان:

- **این احتمال وجود دارد که مقادیری که جهت ذخیره در سلول ها ارسال می شوند، دارای حروف خیلی زیاد یا خیلی کم باشند.**
  - پس در پایانِ Script، جهت یکپارچه سازی ظاهر جدول نهایی، می توان توسط دستور زیر، ابتدا عرض ستون ها را پیدا کرد، و سپس درخواست هماهنگ و مرتبی سازی خودکار عرض ستون ها را دهیم.

```
$usedRange = $Sheet.UsedRange
$usedRange.EntireColumn.AutoFit()
```

- **WorkBook را در یک مکان موردنظر، به شکل یک فایل کامل Excel ذخیره می کنیم:**

```
$workbook.SaveAs("C:\Temp\Test.xlsx")
```

- **از لایه ی Application ای که فراخوانی کرده بودیم، خارج می شویم:**

```
$Excel_Obj.Quit()
```

: Conditional Commands

: If / else

```
if (شرط)
{دستور 1}
else
{دستور 2}
```

مثال:

```
$a1="hi"
if ($a1 -like "his*")
{
Write-Host "it's ok."
}
else
{
Write-Host "It's not ok."
}
```

نکته: برای درج شرطها، حداامکان به جای = از -EQ یا -like و یا مشابه آنها استفاده می کنیم.

مثال: دستور زیر، بررسی می کند که در درایو C پوشه ای به نام Folder2 وجود دارد یا نه، اگر نبود، پیام می دهد: "نیست، ایجادش می کنیم."

```
if(-not (Test-Path -path C:\Folder2))
{
Write-Host "there's no Folder2, we create it ..."
New-Item -Name Folder2 -ItemType Directory -Path c:\
}
Else
{
Write-Host "there is already such a Folder."
}
```

مثال:

```
$a1="ABC"
if($a1 -like "AB*"){
Write-Host "almost"
}
elseif($a1 -in "AB","B"){
Write-Host "almost"
}
elseif($a1 -eq "ABC"){
Write-Host "exactly"
}
else{
Write-Host "there is not!"
}
```

نکته: یکی از کاربردهای جالب دستور IF ، این است که می تواند پُر یا خالی بودن یک متغیر را چک می کند.

مثلاً در پاسخ مثال زیر، NOK ظاهر خواهد شد؛ چون مقداری برای متغیر p تعریف نشده است:

```
$p
if($p)
{
Write-Host "OK"   }
else{
Write-Host "Nok" }
```

و در پاسخ مثال زیر، OK ظاهر خواهد شد. [البته که می توان دستور اجرایی را به جای چاپ کردن OK، چیز دیگری تعریف کرد.]

```
$p="ABC"
if($p)
{
Write-Host "OK"   }
else{
Write-Host "Nok" }
```

: Switch

```
$a1 = "I want the IP."

switch($a1)
{
"I want the date."
{Get-Date}
"I want to list the Folders."
{Get-ChildItem}
"I want the IP."
{Get-NetIPConfiguration}
Default
{Write-Host "Enter a valid input..."}
}
```

گزینه ی **Default** در صورتی اجرا می شود که مقدار متغیر، درون گزینه های **Swtich** موجود نباشد.

: Loop Commands

:Foreach

همانطور که می دانیم، هر متغیر می تواند چندین مقدار دریافت کند.

در درون دستور **foreach**، هریک از مقادیری که درون متغیر **a2** قرار دارند را یکی یکی درون متغیر جدیدی به نام **b1** قرار داده و استفاده می کنیم.

```
$a2 = "ali","reza","omid"
foreach($b1 in $a2){
Write-Host "How are you $b1 ?"
}
```

مثال: فرض کنید که از کاربر، نام و ورزش موردعلاقه اش را می پرسید و می خواهید آنها را اعلام کنید:

```
$ar = @{}
$ar.Add("Reza","tennis")
$ar.Add("Omid","football")
```

- همه ی **Key** ها را یکی یکی درون متغیر **k** می ریزیم.

```
foreach($k in $ar.Keys){
```

- **Value** مربوط به **Key** ها را یکی یکی درون متغیر **V** می ریزیم.

```
$v=$ar.$k
Write-Host "$k be $v Alaghe dare."
}
```

: While

مثال: برای درج اعداد یک تا شش:

```
$a1 =0
while ($a1 -lt 6)
{
$a1+=1
Write-Host $a1
}
```

نکته: البته برای درج اعداد در یک بازه، کافی ست ابتدا و انتهای آنرا درج کنید، با دونقطه میان آنها، و **Enter**! مثلاً:

1..100

: Continue

فرض کنید می خواهیم یک سری خروجی را توسط یک دستور حلقه ای درج کنیم، اما برای یکی از دستورات ورودی، می خواهیم درج نشود:

```
$a1 =0
while ($a1 -lt 15)
{
$a1++
if($a1 -eq 8){Continue}
Write-Host $a1
}
```

: break

فرض کنید می خواهیم یک سری خروجی را توسط یک دستور حلقه ای درج کنیم، اما در صورت ورود یک مقدار خاص، حلقه متوقف شود:

```
$a1 =0
while ($a1 -lt 15)
{
$a1++
if($a1 -eq 8){break}
Write-Host $a1
}
```

: Do - While

به معنای: تا زمانی که هنوز شرط برقرار نشده است.

فرض کنید می خواهیم کاری انجام شود، اما فقط تا زمانی که یک شرط برقرار نشده باشد:

```
$a1 =0
do
{
$a1++
Write-Host $a1
}
while ($a1 -lt 5)
```

: Do – until

به معنای: تا زمانی که هنوز شرط برقرار است.

فرض کنید می خواهیم کاری انجام شود، اما تا زمانی که یک شرط برقرار هست:

نکته: در این دستور، برای شرط، از EQ- استفاده می شود!

```
$a2 =0
Do {
$a2++
Write-Host $a2
}
until ($a2 -eq 6)
```

: Function

دستور

: Send Emails

در **PowerShell** می توانیم پاسخ یک دستور یا **Script** را به یک آدرس **Email**، ارسال کنیم.

```
Send-MailMessage -To "payam.avar@test.de" -Subject “Information test” -Body “This is a test
message.” -SmtpServer “smtp.test.de” -DNO OnSuccess, OnFailure -From “payam_avar@yahoo.com”
```

در حقیقت اگر هم ایمیل مبدا و هم ایمیل مقصد در یک شبکه باشند، به همین سادگی می توان، از این **Script** استفاده کرد که به عنوان مثال، به شکل زیر هم می توان آن را گسترش داد:

```
$D = Get-Date -Format 'dd-MM-yyyy'

$From = "payam_avar@yahoo.com"
$To = "payam.avar@test.de"
$Subject = "Information - $D"
$body = "You see the current information as an attached file.."
$Temp_File = "C:\Tmp\Auslandspersonalliste_$D.xlsx"
$SMTP_Server = "smtp.test.de"

Send-MailMessage -To $To -Subject $Subject -Body $body -SmtpServer $SMTP_Server -Attachments
$Temp_File -DNO OnSuccess, OnFailure -From $From
```

PowerShell Hack :

❖ **حذف یک سری گزینه های خاص** (مثل نام Office، شماره mobile، توضیحات، آدرس Email، عنوان شغلی یا Title و نام Department) **برای همه ی Account هایی که در یک مسیر خاص در Active Directory قرار دارند، و در پایان، غیرفعال کردن آن Account ها:**

```
$OU_Address = "XXX"
$Users = Get-ADUser -Filter * -SearchBase $OU_Address -Properties SamAccountName | select SamAccountName
-ExpandProperty SamAccountName
        foreach ($U1 in $Users) {
        Set-ADUser -Identity $U1 -Clear office, mobile, Description, mail, title, department -Enabled:$false
                                }
```

: Public Commands

PS	CMD Equivalent		Description
Stop-Computer	shutdown /s		خاموش کردن PC
Restart-Computer	shutdown /r		Restart کردن PC
Get-ChildItem	dir	ls	فهرست گیری اطلاعات و فایل های موجود در directory خط فرمان
Get-ChildItem -Path C:\			محتویات آدرس C:\ را نشان می دهد.
get-childitem -attrib h	dir -attrib h	ls -attrib h	فهرست گیری اطلاعات و فایل های موجود در directory خط فرمان همراه با فایل های مخفی
Set-location D:\AB	Cd D:\AB		برای بردن Command Line به درایو D و پوشه ی AB
cls	clear		پاک کردن صفحه
Update-Module			CMDLET ها را به روز می کند.
Get-content A.txt	cat A.txt		نمایش محتوای فایل های متنی
Get-NetAdapter	netsh interface ipv4 show interface		NIC های سیستم را لیست می کند.
Get-NetIPConfiguration	ipconfig		مشخصات NIC ها را نشان می دهد.
Get-NetIPAddress -InterfaceAlias ethernet0			آدرس های مختص به NIC به نام ethernet0 را با جزییات لیست می کند.
Rename-NetAdapter -Name "Ethernet0" -NewName "NIC1"			تغییرنام یک NIC: مثلاً از ethernet0 به NIC1
Test-Connection <IP or Name>	Ping		با ارسال چهار بسته به مقصد، برقراری ارتباط را بررسی می کند.
Test-NetConnection <IP or Name>			برقراری ارتباط با مقصد موردنظر را بررسی می کند و اطلاعات ارتباط را می دهد.
Get-Disk	diskpart	List disk	لیست رسانه های ذخیره سازی را نشان می دهد.
Get-ComputerInfo	Systeminfo		مشخصات و تنظیمات کلی سیستم را نشان می دهد.
Get-WindowsFeature X			بررسی می کند که Feature یا Role مربوط به X نصب است یا نه.
Get-WindowsFeature | Where-Object installed -EQ True			Role ها و Feature های نصب شده را نمایش می دهد.
Get-AppxPackage -AllUsers | Select Name			مشاهده ی نام Application های Default ویندوز
Get-AppxPackage -Name *AppName* | Remove-AppxPackage			برای حذف برنامه های پیشفرض ویندوز
Get-Command -Module dnsserver -Name *record*			نمایش دستورات قابل استفاده در مورد DNS Server و Record ها
Invoke-GPUpdate	gpupdate /force		Group Policy ها را Update می کند.
(Get-ADForest).forestmode			نمایش Forest Functional Level
(Get-ADdomain).domainmode			نمایش domain Functional Level
Start-service XX -confirm	Net start XX		فعالسازی و راه اندازی یک Service
Stop-service XX -confirm	Net stop XX		از کار انداختن یک Service
Set-NetFirewallProfile -Name Private,Domain -Enabled False			غیرفعال کردن Firewall
Get-AdForest			نمایش مشخصات اصلی Forest موجود
Get-VMHost | FL			نمایش لیست مشخصات سیستمی که Host برای VM هاست.
Get-NetTCPConnection			پورتهای باز سیستم را نشان می دهد.
Get-NetRoute	route print	NetStat –r	مسیرهای موجود در سیستم را نشان می دهد.
Get-ADObject -Filter …			در میان همه ی Object های AD جستجو می کند.

: Remote System Management

توسط برخی دستورها می توان یک سری عملیات را بدون اتصال Remote در سیستم های دیگر انجام داد، به شرط اینکه عضو Domain و با حساب .Admin باشیم. مثلاً : برای بررسی اینکه چه Role هایی در کامپیتر Server1 نصب شده اند:

```
Get-WindowsFeature -ComputerName Server1
```

و یا برای اطلاع از وضعیت یک سرویس در آن کامپیوتر:

```
Get-WindowsFeature -ComputerName Server1 -Name *Hyper*
```

1. Single-Use Remote Session :

برای اینکه در سیستم Server2 و یا حتی در یک سیستم غیر سرور عضو شبکه (با حساب Admin)، کنسول PowerShell را باز کرده و یک دستور یا Script را وارد کنیم که بر روی Server1 (و یا حتی بر روی چند Server بطور همزمان)، اجرا شود.

حالت اول:

تنها نیاز به نام یا IP سیستم مقصد خواهیم داشت، و درون {} دستور موردنظر را وارد می کنیم:

```
icm -ComputerName DC1,DC2,DC3 -Command {Install-WindowsFeature dhcp}
```

نکته: به جای icm می توان Invoke-Command درج کرد، و به جای Command می توان ScriptBlock درج کرد. مثال:

```
icm -ComputerName DC1 -ScriptBlock {Set-NetFirewallProfile -Name Private -Enabled False}
Invoke-Command -ComputerName DC1,DC2 -Command {Get-Service dns}
```

حالت دوم:

وقتی بخواهیم یک مجموعه دستور که درون یک فایل PowerShell ذخیره کرده ایم را در Remote System ها اجرا کنیم:

```
Invoke-Command -ComputerName DC1,DC2 -FilePath c:\files\Command.ps1
```

نکته: دستور Invoke از طریق پروتکل HTTP کار می کند.

2. Interactive Remote Session :

برای اینکه در سیستم Server2 و یا حتی در یک سیستم غیر سرور عضو شبکه (با حساب Admin)، کنسول PowerShell را باز کرده و وارد خط دستور سیستم Server1 شویم، طوری که انگار درون کنسول PowerShell مربوط به Server1 هستیم، باید یک Session ایجاد کنیم:

روش اول:

در محیط PowerShell، دکمه های **Ctrl+Shift+R** را زده و نام Server1 و مشخصات Admin User را وارد می کنیم.

و هر دستوری که بخواهیم را وارد می کنیم.

و با درج exit و اینتر، می توان ارتباط را قطع کرد.

روش دوم:

در محیط PowerShell، از دستورات زیر، برای Connection و disconnection یک Session استفاده می شود:

```
Enter-PSSession -ComputerName WDS

Exit-PSSession
```

3. Persistent Remote Session :

یک Session با سیستم مقصد تعریف می کنیم، و آن را درون یک متغیر ذخیره می کنیم:

```
$S1 = New-PSSession -ComputerName WDS
```

برای اینکه مشخصات این Session تعریف شده و یا تمام Session های تعریف شده در این سیستم را مشاهده کنیم:

```
Get-PSSession
```

برای حذف یک Persistent Session :

```
Remove-PSSession $S1
```

برای استفاده از Session تعریف شده:

```
Enter-PSSession -Session $S1
```

مزیت این روش این است که این نوع Session، پایدارتر از روش قبل است.

فرض کنید چندین Session ایجاد کرده ایم و حال قصد حذف همه ی آنها را بطوریکجا داریم:

```
Get-PSSession | Remove-PSSession
```

4. PowerShell Direct :

- این نوع ارتباط، مخصوص ارتباط میان Host و Guest های آن Host در Hyper-V می باشد.
- این قابلیت فقط بر روی Windows 10 و Wndows Server 2016 به بالا وجود دارد.
- هیچ ربطی به نوع Virtual Disk و یا نوع Generation مربوط به VM ندارد.
- در این روش، بدون نیاز به کارت شبکه، می توان به Virtual Machine های موجود، متصل شد.
- این قابلیت، مستقیماً سیستم عامل ها را به یکدیگر متصل می کند.
- پس هیچ الزامی به اینکه سیستم VM دارای NIC بوده و به یک Switch متصل باشد، نخواهد بود.
- تنها باید مشخصات یک حساب مدیریتی Local درون سیستم VM را داشته باشیم.
- VM باید روشن باشد، حتی اگر در حالت sign out هم باشد، مشکلی ندارد، فقط باید روشن باشد.
- دارای دو حالت Interactive و Single-Use هم می باشد.

❖ حالت Interactive :

در سیستم Host و در PowerShell، برای اتصال به یک VM ، از یکی از دو دستور زیر استفاده می کنیم:

```
Enter-PSSession -VMName VMNAME
Enter-PSSession -VMGuid VMGuid
```

نکته: برای مقدار VMName باید نام Virtual Machine، در کنسول Hyper-V را درج کرد.

نکته: برای مقدار VMGuid باید نام VM ID مربوط به VM موردنظر را درج کنیم، که توسط دستور زیر بدست می آید:

```
Get-VM | Select-Object VMName, VMID
```

پس از وارد کردن یکی از دو دستور بالا، برای اتصال، به VM، باید مشخصات یک Admin User <u>Local</u> درون آن VM را وارد کنیم. مثلاً Administrator.

نکته: اگر VM موردنظر، عضو Domain شده باشد، برای مشخصات Local Admin User باید User name را به صورت زیر درج کرد:

Computer Name\Local Admin User Name

مثال:

برای اتصال به یک VM به نام VM1 که متصل به Domain شده است و نام Computer Name آن، DC1 است:

```
Enter-PSSession -VMName VM1
     User name: DC1\Administrator
     Password : XXXXX
```

❖ حالت Single-Use :

مثلاً برای اجرای یک دستور در یک Virtual Machine:

```
Invoke-Command -VMName VM1 -ScriptBlock {Get-ComputerInfo}
```

❖ حالت Persistent :

مثال: برای کپی کردن یک فایل از درون درایو E مربوط به Host، به درایو C مربوط به VM1، به ترتیب زیر عمل می کنیم:

```
$S1 = New-PSSession -VMName VM1
Copy-Item -Path 'e:\File-WDS.txt' -Destination c:\ -ToSession $S1
```

حال برای کپی کردن یک فایل از VM1 به مثلاً درایو E مربوط به Host :

```
Copy-Item -Path 'c:\ File-VM1.txt' -Destination E:\ -FromSession $S1
```

PowerShell DSC :

فرض کنید بخواهیم یک سری تنظیمات را بر روی چند Server عضو Domain انجام دهیم. به طور کلی دو روش خواهیم داشت:

- یکی یکی به هریک از سیستم ها Log in کرده و تنظیمات را انجام دهیم؛ که کار وقت گیر و طاقتفرسایی خواهد بود.
- در یکی از سرورها و از طریق PowerShell عمل کنیم.

پس بطورطبیعی، روش دوم مناسب تر است.

اما از طریق PowerShell نیز باید یک سری کد مربوطه را به ازای هریک از سیستم ها، تنظیم و اجرا کرد!

- در حقیقت سیستم PowerShell دارای یک قابلیت یا ابزار (Extension) به نام DSC (Desired State Configuration) می باشد که توسط آن، تنظیمات موردنظر را به شکل یک سری Script درون یک بسته با پسوند mof. درج می کنیم.
- حال به سادگی می توان این بسته را بطورمستقیم و همزمان، به همه ی سیستم ها ارسال کرد.

این بسته ی Script، که اطلاعات هیچیک از Server ها را ندارد، چگونه در هریک از آنها اجرا و اعمال می شود؟!

- در حقیقت هریک از Server ها دارای یک ابزار هستند به نام LCM (Local Configuration Manager) که اطلاعات آن Server را درون بسته ی Script دریافتی، پیکربندی می کنند تا سپس آنرا اجرا کنند.

LCM دارای سه حالت یا Mode است:

- **Deploy** : فقط تنظیمات را اعمال و نتیجه را اجرا می کند.
- **Deploy and Monitor** : علاوه بر اجرای تنظیمات، همچنین اگر تنظیمی مشکل داشته باشد یا تغییر کرده باشد، گزارش می دهد.
- **Deploy and Auto Correct** : برحسب فواصل زمانی معین، فایل Script را چک می کند و اگر تغییری یا ایرادی پیش آمده باشد، دوباره آنرا بطورخودکار به حالت ابتدایی که دریافت کرده بود، بر می گرداند.

ما می توانیم این ابزار LCM را نیز Config کنیم.

- می توانیم میزان بازه ی زمانی برای چک کردن تنظیمات Script را تعیین کنیم. (حداقل 15 دقیقه)
- می توانیم Mode کارکرد LCM را تنظیم کنیم.

اما اینکه آن بسته ی Script چگونه به دست هریک از Server ها برسد، به این بستگی دارد که آنها را در چه Mode ای تنظیم کرده باشیم:

- **Push** : در این حالت، سیستم موردنظر منتظر می ماند که Server اصلی شبکه، آن بسته را به سمت او ارسال کند.
- **Pull** : در این حالت، به محض وجود یک بسته ی Script با پسوند mof، در Server اصلی، اقدام درخواست و دریافت آن می کند.

فرض کنید نیاز باشد که در تنظیمات بسته ی Script، یک تغییر کوچک اعمال شود.

پس فایل را اصلاح می کنیم.

در حالت Push، آن را دوباره به Server یا Server های موردنظر ارسال می کنیم.

در حالت Pull، سیستم موردنظر، بر طبق زمانبندی ای که دارد، Server اصلی را چک می کند و وقتی متوجه آن شد، آن را دریافت می کند.

اما در Server مقصد پس از دریافت فایل جدید، نیازی نیست که همه ی تنظیمات موجود در Script اجرا شوند، بلکه تنها تغییرات اعمال شده را اجرا می کند؛ که به این شیوه، Idempotent گفته می شود.

حالت Push :

در حقیقت برای درج و پیکربندی فایل DSC، نیاز به مقداری برنامه نویسی تحت PowerShell خواهیم داشت.

در ابتدا برای این Script، توسط دستور زیر، یک نام تعیین می کنیم:

```
Configuration Name1{
```

برای وارد کردن نام کامپیوترها، نیاز به یک متغیر از نوع String خواهیم داشت ، با یک نام دلخواه.

تعریف متغیرها، یک پارامتر محسوب می شود، پس ابتدا یک () Param ایجاد می کنیم:

```
Param(
[String[]] $ComputerName="DC4"
)
```

البته می توانستیم نام تعداد بیشتری از کامپیوترها را نیز وارد کنیم:

```
Param(
[String[]] $ComputerName="DC1"."DC4"."DC5"."DC6"
)
```

حال باید دستورات نصب Role یا Feature های موردنظر را وارد کنیم.

- مثلا برای نصب Feature مربوط به IIS:

```
Node $ComputerName{
WindowsFeature IIS
Ensure = "Present"
Name = "Web-Server"
}
```

برای دریافت نام دقیق WindowsFeature: نام همه ی آنها را در Server Manager>Tools می بینیم.

برای دریافت نام دقیق Name، می توانیم در PowerShell دستور Get-WindowsFeature را بزنیم.

- برای حذف Role یا Feature های بالا:

```
Node $ComputerName{
WindowsFeature IIS
Ensure = "Absent"
Name = "Web-Server"
}
```

مثلاً برای نصب IIS، همراه با یک Feature مربوط به Web Management، فایل نهایی بصورت زیر می شود:

```
Configuration Name1
{
Param(
[String[]] $ComputerName="DC1"."DC4"."DC5"."DC6"
)
Node $ComputerName
{
WindowsFeature IIS{
Ensure = "Present"
Name = "Web-Server"
                    }
WindowsFeature IISManagement {
Ensure = "Present"
Name = "web-mgmt-service"
DependsOn = @("[WindowsFeature]IIS")
                                    }
}         }
```

دستور dependson مشخص می کند که این Feature چه پیشنیازهایی دارد.

درون []، نوعِ پیشنیاز را مشخص می کند.

مثال:

می خواهیم از درون سیستم DC1، بر روی DC2 سرویس IIS را همراه با Feature مربوط به **Web Management** نصب کنیم:

1. درون **PowerShell** سیستم **DC1** دستورات نصب سرویس **IIS** را وارد می کنیم.

اما قبل از دستورات نصب، می توانیم درون خودش، تنظیمات **LCM** را نیز درج کنیم:

```
Configuration Name1
{
Param(
[String[]] $ComputerName="DC2"
)
Node $ComputerName
{

LocalConfigurationManager {
ConfigurationMode = "ApplyAndMonitor"
ConfigurationModeFrequencyMins = 45
RebootNodeIfNeeded = $false
RefreshMode = "Push"
}

WindowsFeature IIS{
Ensure = "Present"
Name = "Web-Server"
                  }
WindowsFeature IISManagement {
Ensure = "Present"
Name = "web-mgmt-service"
DependsOn = @("[WindowsFeature]IIS")
                              }

Registry remotemanagement {
Key = "HKLM:\SOFTWARE\microsoft\webmanagement\Server"
ValueName = "EnableRemoteManagement"
ValueType = "Dword"
ValueData = "1"
DependsOn = @("[windowsfeature]IIS","[WindowsFeature]IISManagement")
                           }

Service WMSVC{
Name = "wmsvc"
StartupType = "Automatic"
State = "Running"
DependsOn = "[Registry]RemoteManagement"
              }

}

}
```

2. تمام این کد را انتخاب کرده و **Run** می کنیم.

پس درون حافظه ی **RAM** سیستم ذخیره می شود.

حال باید این فایل را ذخیره و یکبار **Compile** کنیم، پس درج می کنیم:

```
Name1 -ComputerName DC2 -OutputPath "c:\Folder1"
```

اگر بیش از یک کامپیوتر مقصد وجود داشت، نام آنها را با , از یکدیگر جدا می کردیم، و در نتیجه در آدرس مشخص شده، به ازای هر کامپیوتر، یک فایل **Script** ایجاد می شد.

- برای تنظیمات **LCM** یک فایل جدا ایجاد می شود.

3. ابتدا فایل **LCM** را ارسال و تعریف می کنیم:

```
Set-DscLocalConfigurationManager -Path "C:\Folder1"
```

4. حال باید این فایل (یا فایل های) **Script** را به سیستم های مقصدی که نام شان را تعریف کردیم، ارسال و نصب کنیم:

```
Start-DscConfiguration -path "c:\Folder1" -wait -verbose
```

5. برای مشاهده ی تنظیمات **DSC Config.** و تنظیمات **LCM**، می توانیم در سیستم مقصد دستورات زیر را به ترتیب وارد کنیم:

```
Get-DscLocalConfigurationManager
Get-DscConfigurationStatus
```

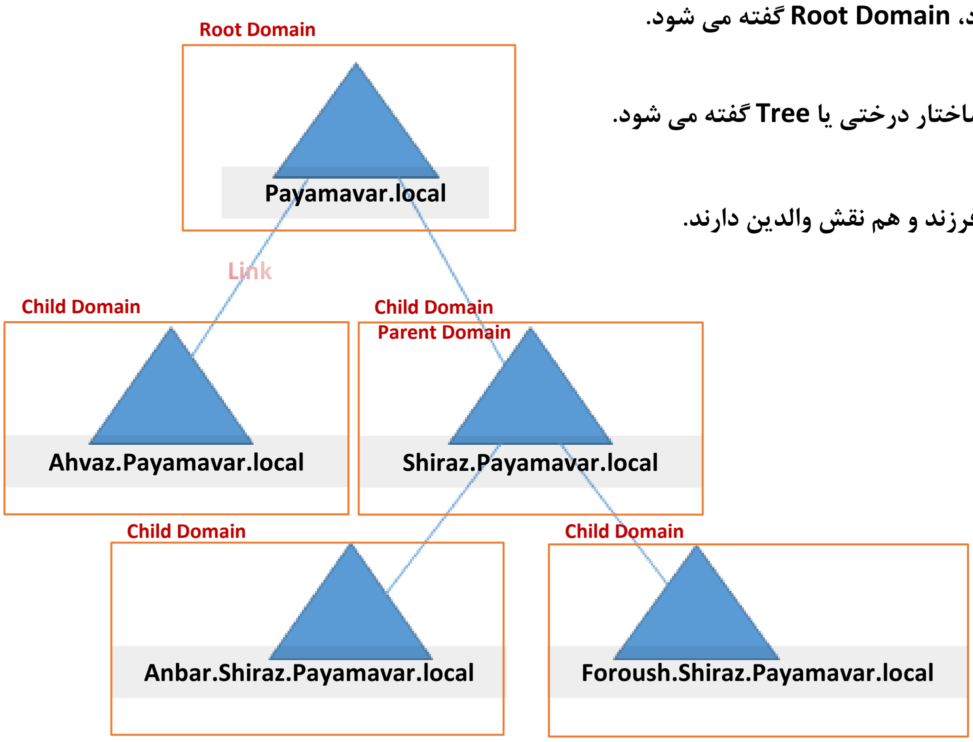
6. برای مشاهده ی روشن یا قطع بودن **DSC** در سیستم مقصد درج می کنیم:

```
Test-DscConfiguration
```

:Domain

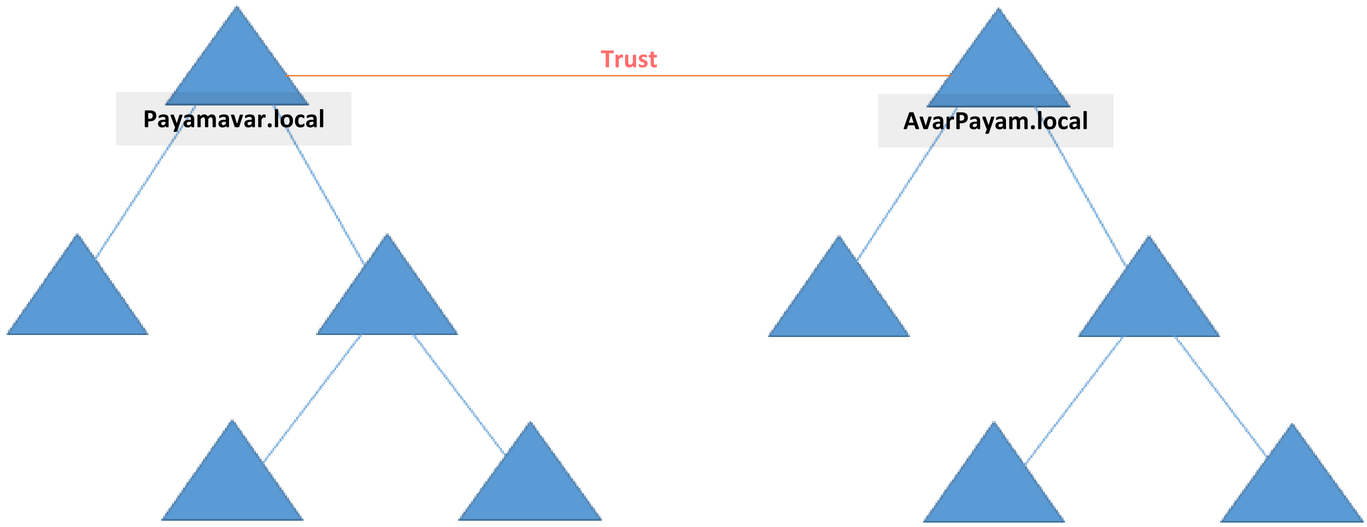
هرکجا که کامپیوترها از یک ساختار نامگذاری سلسله مراتبی استفاده می کنند، آنجا از یک **Domain** بهره برده می شود.
به اولین **Domain** ای که ساخته می شود، **Root Domain** گفته می شود.

- به این ساختار سلسله مراتبی، ساختار درختی یا **Tree** گفته می شود.
- **Domain** های میانی، هم نقش فرزند و هم نقش والدین دارند.



- به **Child Domain** ها، **Subdomain** هم گفته می شود.
- **Child Domain** ها به **Parent Domain** ها دسترسی ندارند، اما **Parent** ها کاملا به **Child** ها دسترسی دارند.
- همه ی کاربرانِ هریک از **Domain** ها، قادر به **login** یا ورود به سیستم، در تمام **Domain** های دیگر هستند.
- در حقیقت ساختار **AD** از ساختار نامگذاری **DNS** برای ساختار درختی خود استفاده می کند که چیزی شبیه به همان ساختار نامگذاری است که توسط **Website** ها استفاده می شود.

- فرض کنید که دو **Tree** داشته باشیم، و با اتصال **Root Domain** آنها به یکدیگر، آنها را به هم مرتبط کنیم.
- به کل همبندی این شبکه ها، **Forest** گفته می شود.
- به لینک ارتباطی بین **Tree** ها، **Trust** گفته می شود.



با ایجاد یک Domain Controller تنها و ساده، فوراً به شکل خودکار، ساختار کلی Domain Controller و Tree و Forest در Domain تشکیل خواهند شد.

انواع روش های طراحی Forest :

- Single Domain : وقتی Forest تعریف شده در سیستم، فقط یک Domain داشته باشد.
- Multi Domain : وقتی Forest شامل چند Domain باشد.که در این حالت همیشه رابطه ی Domain ها با هم، به شکل Parent و Child است.
- Multi Tree : دارای چندین Domain است که در Tree های مختلف قرار دارند.

: Active Directory

Active Directory یک Database از کلیه ی اطلاعات زیرساختیِ شبکه است.

Active Directory پنج سرویس اصلی دارد :

1. AD DS : Active Directory Domain Services :

- در حقیقت یک وظیفه یا role است که می توان آن را در سیستم Server نصب کرد تا بتوان توسط آن، اعضای شبکه را به شکل فراگیر، کنترل و مدیریت کرد. اولین و مهم ترین کاربرد این سرویس، عمل Authentication است.
- سیستمی که نقش AD DS روی آن نصب می شود، Domain Controller (DC) نامیده می شود.
- AD DS از پروتکل های Kerberos و LDAP و DNS استفاده می کند.
- ترافیک AD DS با پروتکل LDAP روی پورت TCP 389 منتقل می شود.

2. AD FS : Active Directory Federation Services :

توسط این Service تمامی Client های شبکه ی جاری، توسط Account ای که در همین شبکه دارند، قادر به دسترسی به یک Software در یک شبکه ی دیگر خواهند بود.

3. AD CS : Active Directory Certificate Services

4. AD RMS : Active Directory Right Management Services

5. AD LDS : Active Directory Lightweight Directory Services

: Domain Terms

- Security boundary : به محیطی که در شعاع کنترل یک Domain است گفته می شود.
- Object : به تک تک اعضای فیزیکی و غیرفیزیکی تشکیل دهنده ی شبکه، Object گفته می شود. User، Computer و ... .
- Attribute : هر Object دارای یک یا چند صفت است. بعنوان مثال، یک user دارای صفاتی مثل first name، last name، password و ... می باشد. حتی نوع و نام سیستم عامل یک کامپیوتر نیز Attribute می باشند.

- Schema : پایگاه داده ای است که اطلاعات تمام آبجکتهای AD DS همراه با Attribute های را درون خود ذخیره می کند.
- Site : یک مفهوم Logical است که به یک مفهوم Physical یعنی مکان، اشاره می کند.
- مثلاً یک شرکت بزرگ، دارای شعبی در چند شهر، و یا دارای چند شعبه در یک شهر است، هر کدام از این شعب، یک Site هستند.

در AD باید ارتباط میان تمام Site های شبکه برقرار باشد.
به محض راه اندازی اولین Domain Controller ، یک Forest و یک Site (پیشفرض به نام Default-First-Site-Name) بوجود می آید.
اگر در آینده قصد ایجاد یک Site جدید را داشته باشیم، باید این نام پیشفرض اولین سایت را تغییر دهیم.

- Subnet : در اولین شبکه، حداقل یک Subnet وجود دارد. که البته می توان ده ها و صدها Subnet هم داشت. توصیه می شود که Site های مختلف شبکه، دارای Subnet های متفاوت باشند.

- Stand-alone Server : ویندوز سروری است که Domain Controller روی آن نصب نشده است.

:Setup a Server

اگر در هنگام نصب ویندوز Server، یکی از گزینه های Windows Server یا Windows Server Core installation را انتخاب کنیم، نسخه ی Core ویندوز را نصب می کند که برای کنترل آن قادر و مجبور خواهیم بود، تنها از محیط Command Prompt عمل کنیم.

اگر نسخه ی Windows Server (Desktop Experience) یا Windows with GUI را انتخاب کنیم، درست مثل یک ویندوز معمولی با ظاهر گرافیکی خواهد بود.

:Server Core Windows Promotion

این نسخه از ویندوز Server، یک سری مزیت ها دارد:

- سبک تر از نسخه ی graphical است، که در نتیجه سریع تر عمل خواهد کرد.
- می تواند با مقدار Ram کمتری کار کند.
- به حجم کمتری از حافظه جهت نصب و Implementation نیاز دارد.
- مثل نسخه ی گرافیکی، نیاز به Update ندارد.

مراحل ابتدایی نصب، کاملاً مشابه می باشند.

پس از نصب ویندوز Server، فقط یک محیط dos با محیط مشکی و یک دایرکتوری از درایو ویندوز ظاهر می شود.

Alt+Ctrl+Delete را می زنیم.

برای تعیین یک رمز عبور، OK را زده و یک پسورد تعریف می کنیم.

لازم است که به محیط کنترل و تنظیم Server به نام Server Configuration برویم که یک صفحه ی آبی رنگ خواهد بود.

یا درج و Enter می کنیم : sconfig

و یا به آدرس زیر رفته و فایل sconfig.cmd را باز می کنیم:

C:\windows\system32\sconfig.cmd

همانطور که می بینیم، برای هریک از تنظیمات، یک شماره وجود دارد، که با درج آن شماره و Enter، می توانیم آنها را پیکربندی کنیم.

1. به ترتیب اقدامات زیر را تحت dos انجام خواهیم داد:
   - تغییرنام Computer
   - فعال سازی Remote desktop
   - Power Plan را برای Sleep و Turn Off بر روی Never قرار می دهیم.
   - Date and Time را تنظیم می کنیم.
   - یک IP به صورت Static و نه از DHCP ، به سیستم اختصاص می دهیم.و سپس آدرسی برای DNS تعیین می کنیم.
   - وارد Network Setting می شویم.
   - گزینه ی Set Network Adapter Address را انتخاب می کنیم.
   - S را برای Static انتخاب می کنیم.
   - بر اساس Range ای که Default Gateway دارد، یک IP وارد می کنیم.
   - برای Subnet mask می توانیم آن را در همان Class C رها کنیم.

- پس از تعیین DNS، از این محیط خارج شده و به cmd برگشته و به آدرس DNS و آدرسی که برای کامپیوتر تعیین کرده بودیم ping می کنیم تا از صحت آنها مطلع شویم.

نکته: با درج Powershell و یا Start Powershell می توانیم به محیط آن برویم.

برای تعیین آدرس IP و DNS، به کمک دستورات زیر در محیط cmd هم می توان عمل کرد.

- ابتدا با دستور زیر نام Adapter های کارت شبکه ی این سیستم را پیدا می کنیم:

```
Netsh Interface Show Interface
Netsh Interface Ipv4 Set Address Name="Ethernet" static 192.168.139.139  255.255.255.0  192.168.139.1
```

IP اول: آدرسی برای این سیستم
IP دوم: آدرس Subnet mask آن
IP سوم: آدرس Gateway آن

به صورت زیر دو آدرس DNS تعریف می کنیم:

```
Netsh Interface Ipv4 Set DNS Name="Ethernet" static 192.168.139.139
Netsh Interface Ipv4 Set Address Name="Ethernet" static 8.8.8.8 index=2
```

برای مشاهده ی تنظیمات NIC در cmd:

```
ipconfig
```

برای مشاهده ی تنظیمات NIC در PowerShell از یکی از دستورات زیر:

```
Get-NetIPConfiguration
Get-NetIPAddress -InterfaceAlias NICName
```

برای تعیین آدرس IP و DNS، به کمک دستور زیر در محیط PowerShell هم می توان عمل کرد.

- با درج Powershell و یا Start Powershell به محیط آن می رویم.
- با دستور زیر نام Adapter های کارت شبکه ی این سیستم را پیدا می کنیم:

```
Get-NetAdapter

New-NetIPAddress -InterfaceIndex 8 -IPAddress 192.168.139.139 -PrefixLength 24 -DefaultGateway 192.168.139.139

Set-DnsClientServerAddress -InterfaceIndex 8 -ServerAddresses ("192.168.139.139","8.8.8.8")
```

نکته: در PowerShell، برای تنظیم آدرس Default Gateway برای Adapter ای که آدرس IP را از قبل دریافت کرده است، باید ابتدا یکبار تنظیم را به اتوماتیک برگرداند و سپس از اول دستور را کامل وارد کرد.

```
Set-NetIPInterface -InterfaceAlias 'Ethernet 3' -Dhcp Enabled
New-NetIPAddress -InterfaceIndex 4  -IPAddress 10.10.0.15  -PrefixLength 24  -DefaultGateway 10.10.0.1
```

2. Disk ها و Drive ها را بررسی می کنیم.

- برای کار بر روی محتویات درون Drive ها، می توانیم از طریق Diskpart و سپس List disk، ابتدا محتویات آنها را بررسی کرد؛ و یا از طریق یکی از دستورات زیر، آنها را همراه با حرف نامشان مشاهده کرد:

```
cmd:          wmic logicaldisk get name, description, volumename
PowerShell :  Get-PSDrive -PSProvider FileSystem
```

با توجه به اینکه معمولاً Server اصلی شبکه را به صورت GUI راه اندازی می کنیم، و Server های Core، اعضای فرعی، با وظایف منحصربفرد خود هستند، برای نصب و راه اندازی Role ها بر روی Server Core ها، می توان در Server اصلی شبکه، بر روی نام Server های Core کلیک راست کرده و Add Roles and Features را زد.

: Turn off the Firewall

در PowerShell توسط دستور زیر، از وضعیت Firewall استعلام می گیریم.

```
Get-NetFirewallProfile
```

- توسط دستور زیر Firewall را در هرسه حالت آن، خاموش می کنیم.(می توان فقط یکی یا دو حالت را درج کرد)

```
Set-NetFirewallProfile -Profile domain,private,public -Enabled False
```

:Time Zone and Date

1. ابتدا توسط دستور زیر Time Zone جاری را مشاهده می کنیم:

```
Get-TimeZone
```

2. اگر Time Zone اشتباه بود، آن را تنظیم می کنیم، اما ابتدا باید مشخصات دقیق Time Zone صحیح را بدانیم، درج می کنیم:

```
Get-TimeZone -ListAvailable
```

3. توسط دستور زیر، Time Zone را تصحیح می کنیم:

```
Set-TimeZone -Id "W. Europe Standard Time" -PassThru
```

- برای مشاهده ی Time Zone در cmd، درج می کنیم: tzutil /l

: Define a NTP Server

- ✓ در گوگل آدرس Time Server ها را جستجو می کنیم و یکی از نزدیکترین ها را (از نظر جغرافیایی) انتخاب می کنیم.
- ✓ وارد محیط PowerShell (با دسترسی Administrator) شده و تایپ می کنیم:

```
w32tm.exe /config /manualpeerlist:"ptb.time1.ptb.de" /syncfromflags:manual
```

باید پیغام زیر ظاهر شود:

```
The command completed successfully
```

- اگر بخواهیم چندین NTPserver را به سیستم معرفی کنیم که زمان را طبق همه ی آنها تنظیم کند به شکل زیر عمل می کنیم:

```
w32tm.exe /config /manualpeerlist:"ptb.time1.ptb.de ptb.time2.ptb.de ptb.time3.ptb.de" /syncfromflags:manual
```

- ✓ حال برای اینکه time server جدید بکار بیفتد، لازم است که یکبار time server را قطع و وصل کنیم.

پس به ترتیب دستور های زیر را یکی یکی وارد کرده و enter می زنیم:

```
Stop-Service W32Time
Start-Service W32Time
```

- ✓ حال برای اینکه گزارش بگیریم ببینیم NTPserver بر روی کدام گزینه تنظیم شده است، وارد می کنیم:

```
w32tm /query /configuration
```

در نتایج باید خط زیر یا خط زیرین آن را دریافت کنیم:

```
NtpServer: ptb.time1.ptb.de (Local)
NtpServer: ptb.time1.ptb.de ptb.time2.ptb.de ptb.time3.ptb.de (Local)
```

: Windows Update

به ترتیب دستورهای زیر را وارد می کنیم:

```
Set-ExecutionPolicy RemoteSigned

Install-Module PSWindowsUpdate

Import-Module PowerShellGet

Get-WindowsUpdate

Install-WindowsUpdate
```

نکته:

اگر با خطایی مبنی بر پکیج NuGet مواجه شدیم، به ترتیب دستورات زیر را وارد می کنیم:

```
[Net.ServicePointManager]::SecurityProtocol
[Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor
[Net.SecurityProtocolType]::Tls12
[Net.ServicePointManager]::SecurityProtocol
Register-PSRepository -Default -Verbose

Set-PSRepository -Name PSGallery -InstallationPolicy Trusted

Install-PackageProvider -Name NuGet -Force -Debug -Verbose
Install-Module -Name PowerShellGet -Force -Verbose -Debug
Update-Module -Name PowerShellGet -Force -Verbose -Debug
```

: GUI Windows Promotion

پس از نصب ویندوز Server، باید یک سری تنظیمات اولیه ی محیط ویندوز را انجام دهیم.

1. Firewall را برای شبکه ی داخلی inactive می کنیم.

در Run تایپ می کنیم: firewall.cpl

وارد گزینه ی turn windows firewall on or off می شویم.

و در قسمت Private گزینه ی turn off win... را انتخاب کرده و Ok می کنیم.

2. Remote Desktop را active می کنیم.

وارد مسیر زیر می شویم:

Control Panel > System > Advanced system Settings

3. Power Plan را از کار می اندازیم.

وارد مسیر زیر می شویم:

Control Panel > Power Options

روی گزینه Change plan settings روبروی گزینه ی فعال فعلی، کلیک می کنیم.

همه ی گزینه ی Turn off و Sleep را روی Never قرار می دهیم.

4. تنظیمات ظاهری را بر حسب high speed قرار می دهیم.

حال در قسمت Performance وارد Setting و تب Visual Effects شده و از گزینه های این تب، یکی از گزینه های زیر را انتخاب کنیم:

Let windows choose what's best for my computer
Adjust for best performance

وارد تب Advanced شده و گزینه ی Background Services را فعال می کنیم.

5. در همین تب، در بخش virtual memory وارد گزینه ی Change شده و گزینه ی Custom size را فعال کرده و مقادیر initial و maximum را عددی برحسب گیگابایت تعیین می کنیم.

مقدار این عدد، باید یک و نیم برابر مقدار Ram سیستم باشد.مثلاً برای Ram 4Gig این مقدار را 6000 در نظر می گیریم.

برای سیستم هایی که مقدار تبادلات داده ایه زیادی دارند، این مقدار را کمتر هم در نظر می گیریم، مخصوصاً Server های پرکار یا سیستم هایی که دستگاه های ذخیره سازی نه چندان قوی ای دارند؛ چون حجم زیاد برای فایل Paging، باعث کند شدن سیستم نیز می شود.

6. Automatic Services را اجرا می کنیم.

پنجره ی Services را باز کرده و چک می کنیم که همه ی سرویس هایی که دارای Startup Type با مقدار Automatic هستند، باید در حالت Running قرار داشته باشند.(با کلیک راست بر روی آن و انتخاب Start)

7. یک Static IP مناسب برای این کامپیوتر تنظیم می کنیم.

به تنظیمات Ethernet سیستم رفته و یک IP ثابت در یک محدوده ی مناسب و برنامه ریزی شده، وارد می کنیم.

برای دو آدرس DNS، یکبار همان IP خودش یا IP Loopback (127.0.0.1) را و برای دیگری، مثلاً 8.8.8.8 را وارد می کنیم.

- تمامی سرویس دهنده ها در یک شبکه، باید دارای یک IP Static باشند.

مثل انواع سیستم های Server ، Modem ها و Printer ها.

پس لازم است تا IP همه ی سرویس دهنده ها را به شکل Manual تنظیم کنیم.

8. اتصالات شبکه را چک می کنیم.

با Ping به آدرس **localhost** و آدرس **Gateway** و یک آدرس اینترنتی، اتصالات **TCP-IP** و اینترنت را چک می کنیم.

9. گزینه های غیرضروری **Taskbar** را غیرفعال می کنیم.

بر روی **Taskbar** کلیک راست کرده و وارد **Setting** شده و پایین آمده و وارد **Turn System Icons On or Off** می شویم. می توانیم **Volume** و **Location** و ... را **Off** کنیم.

10. زمانبندی سیستم را تنظیم می کنیم.

✓ پنجره ی **Adjust Date/Time** می شویم:

- گزینه ی **Set Time Automatically** فعال باشد و
- گزینه ی **Set Time Zone Automatically** غیرفعال باشد،
- **Time Zone** را بر اساس منطقه ی جغرافیایی که در آن قرار داریم انتخاب می کنیم،
- **adjust for daylight saving time automatically win 10** را نیز فعال می کنیم.
- یکبار **Restart** می کنیم.

11. **NTP Server** را مشابه با حالت **Server Core** تعریف می کنیم.

12. **Windows** را **Update** می کنیم.

- می توان با وارد کردن کلمه ی میانبور زیر در **Run** به صفحه ی آن رفت:

ms-settings:windowsupdate

نکته: اگر ویندوز **Server** جاری، فاقد یک **License** معتبر است، **Update Service** را در ویندوز قطع می کنیم یا می بندیم:

وارد کنسول **Services** شده و وارد **Properties** گزینه ی **Windows Update** شده و آن را **Stop** کرده و **Startup Type** آنرا بر روی **Manual** قرار می دهیم.

13. **Windows** را **Activate** می کنیم.

14. گزینه ی **IE ESC** را غیرفعال می کنیم.

وارد **Server Manager** شده و در تب **Local Server**، گزینه ی **IE Enhanced Security** را باز کرده و آن را برای **Administrators** در حالت **OFF** قرار می دهیم.

: Installation Active Directory

1. در پنجره ی System یک نام مناسب برای Computer Name انتخاب می کنیم.
2. در پنجره ی Server Manager روی Manage زده و Add Roles and Features را باز می کنیم.

در ویزارد نصب، به جز اینکه گزینه های **Active Directory Domain Services** و **DNS Server** را باید انتخاب کنیم، تغییر خاصی نیاز نیست و نصب را به پایان می رسانیم.

در حقیقت، برای ایجاد یک شبکه، از همان ابتدا، چهارچوب آن را آماده ی تبدیل شدن به یک Forest می کنیم.

از طریق PowerShell هم می توان:

```
Install-WindowsFeature ad-domain-services -IncludeAllSubFeature -IncludeManagementTools
Install-WindowsFeature DNS -IncludeAllSubFeature -IncludeManagementTools
```

3. پس از نصب در قسمت Notifications ، روی گزینه ی Promote this server to a Domain Controller کلیک می کنیم.

با سه گزینه مواجه می شویم:

✓ Add a domain controller to an existing domain :

زمانی که یک Domain ایجاد کرده ایم و موجود و بکار است، و قصد داشته باشیم یک Domain کمکی (Additional Domain) برای آن تعیین و ایجاد کنیم، به دلایل زیر:

- به جهت Redundancy یا همان High Availability
- بالاتر رفتن سرعت Authentication در شبکه:

  اعضا، فورا به دردسترس ترین Domain وصل شده و احراز هویت می شوند.
- به جهت Load Sharing :

  یعنی برای تقسیم Work Load شبکه از روی یک Domain بر روی دو یا چند Domain.

✓ Add a new domain to an existing forest :

به اهداف زیر، این گزینه را انتخاب می کنیم:

اگر یک Domain ایجاد کرده باشیم و بخواهیم آن را به عنوان Child تعریف کنیم.

اگر بخواهیم یک Tree دیگر را به Tree موجود، متصل کنیم.

✓ اگر اولین بار است که یک DC می سازیم، پس گزینه ی Add a new Forest را انتخاب کرده و برای Name آن، یک نام درج می کنیم.

اما به چه شکل؟!

- نام Domain باید همیشه همراه با یک نام به عنوان ریشه ی تمام Tree باشد.

  یعنی یک پسوند که نشانه ی ریشه ی DC است که این ریشه را توسط یک نقطه، از نام شبکه ی Domain جدا می کنیم.

  بطور معمول، برای نام ریشه در یک شبکه، کلمه ی local را در نظر می گیرند. مثلاً یک Domain با نام payamavar:

payamavar.local

- ما می توانیم یک Domain Name که در تمام محیط Internet یکتا باشد، خریداری کنیم، مثلاً: payamavar.com

- در تب بعد، باید functional level را تعیین می کنیم که در این مورد است که اعضای دیگر شبکه، با چه سیستم عامل هایی قابل قبول برای عضویت در این Domain می باشند.با انتخاب هریک از گزینه ها، در حقیقت سطح کاربری این Domain ای که در حال ایجاد آن هستیم را پایین می آورد تا با سیستم های دیگری که آن ویندوزها را دارند، سازگاری داشته باشد.

مثلاً اگر windows server 2016 را انتخاب کنیم، در آینده اگر یک Domain با ویندوز سرور 2008 بخواهد عضو شبکه شود، قادر نخواهد بود!

اگر در ویندوز سرور 2016 ، سطح functional level را مثلاً روی 2012 قرار دهیم، در حقیقت از قابلیت هایی که در ویندوز 2016 هستند برخوردار نخواهیم بود، چون سطح قابلیت های آن را تا 2012 پایین آورده ایم که با اعضای شبکه ای که ویندوز قدیمی تر تا 2012 دارند نیز سازگار باشد.

چنانچه تمام DC های Forest دارای ویندوز سرور 2016 باشند و فقط یکی از آنها دارای ویندوز 2008 باشند، باید Forest Functional Level را روی Windows 2008 تنظیم کنیم.

- در آینده می توان این functional level را ارتقا داد، اما امکان پایین آوردن آن وجود ندارد!
- البته تنها زمانی می توان Functional Level را افزایش داد که تمام Domain Controller های شبکه، نسخه یا نسخه هایی از ویندوز Server را داشته باشند که بتوانند از Functional Level جدید پشتیبانی کنند.
- در موارد مجاز، بازگشت به Functional Level پایین تر، فقط از طریق Powershell ممکن است. چه برای Domain Functional Level، و چه برای Forest Functional Level.

✓ با فعال کردن تیک DNS Server ، این قابلیت را نیز برای این Domain فعال می کند.
✓ با توجه به اینکه در حال ایجاد یک Forest هستیم، پس باید Global Catalog را نیز فعال کنیم.

از نظر امنیتی توصیه می شود که مسیر ذخیره سازی فایل های Sysvol و بقیه ی فایل های سرویس AD را به درایوی غیر از درایو C تغییر دهیم و از لحاظ Permission ها، روی Folder فوق هم تمام موارد امنیتی لازم را رعایت کنیم تا مهاجمین نتوانند به این فایل ها دسترسی داشته باشند.
البته درایوی که این فولدرها را در آن قرار می دهیم باید حتما دارای فایل سیستم NTFS باشد تا بتوان از مجوزهای NTFS نیز استفاده کرد.

- فرض کنیم که بعداً قصد داشته باشیم تمام تنظیمات DC را Reset کنیم، پس یک پسورد (DSRM) انتخاب می کنیم که قبل از Reset درخواست خواهد شد.

✓ در ادامه، خود سیستم بطورخودکار، یک نام مناسب و معتبر، برای NetBiosName پیدا کرده و نشان می دهد که می توان در همینجا آن را تغییر داد. این یک نام خلاصه اما کارآمد برای Domain خواهد بود. (تقریباً مثل یک نام مستعار مشخص و قابل شناسایی)

✓ و Install را زده و در پایان، سیستم باید یک بار Restart شود تا DC فعال شده و محیط، تبدیل به یک محیط دومینی شود.

نکته: تمام این نصب و Domain Implementation و ابزارهای Active directory را می توان در محیط Power Shell هم انجام داد.

SYSVOL (System Volume) و NETLOGON :

یکی از کاربردهای ظاهری که این دو پوشه دارند، این است که از طریق آنها متوجه شویم که AD درست بر روی Windows Server نصب شده است.
پس در Server و در CMD ، دستور net share را وارد می کنیم تا در پاسخ، پوشه های share شده ی این ویندوز را دریافت کنیم.
اگر در پاسخ، پوشه های sysvol و netlogon دریافت شوند، به معنای نصب صحیح AD می باشد.

در حقیقت Client های موجود در شبکه، از طریق استفاده از پوشه های NETLOGON و SYSVOL می توانند به دستورات و فرمان ها و داده هایی که Server در اختیار آنها قرار می دهد دسترسی پیدا کنند.

پوشه ی SYSVOL یکی از مهمترین بخش های Active Directory محسوب می شود.
اگر SYSVOL نباشد، کلاینت ها و DC های موجود در Domain، قادر به update و Access اطلاعاتِ Domain نخواهند بود.
مدیریت و Replication پوشه ی SYSVOL، توسط یک سرویس به نام DFS Replication انجام می شود.
پوشه SYSVOL بر روی تمامی DC های موجود در یک مجموعه ی Domain وجود دارد و برای محافظت بهتر از آن، بر روی یک درایو از سیستم قرار می گیرد که فایل سیستم آن NTFS باشد.
تمامی Policy هایی که شما در یک Domain ایجاد می کنید و به ویژه Policy های مربوط به DC ها و همچنین Logon Script هایی که بایستی بر روی اعضای دامین اجرا شوند در این پوشه قرار دارند.

پوشه ی Netlogon به عنوان پشتیبان پوشه ی Sysvol کار می کند.

- ✓ **یک تفاوت یا کاستی در Windows Server نسبت به Windows Client این است که وقتی در Server ، روی آیکون My Computer کلیک راست کرده و Manage را می زنیم، پنجره ی Server Manager باز می شود. و برای باز کردن Computer Management :**
  - **بر روی Start کلیک راست کرده و آنرا انتخاب می کنیم.**
  - **در Run : compmgmt.msc**
  - **در پنجره ی Server Manager و از گزینه ی Tools آن را انتخاب می کنیم.**

- ✓ **یک تفاوت یا کاستی دیگر در Domain Controller، نسبت به همه ی سیستم های دیگر، این است که وقتی در DC، وارد Computer Management می شویم، گزینه ی Local Users and Groups وجود ندارد و کاملاً حذف شده است.**

: DSRM password recovery

در صورت فراموش کردن رمز عبور حساب local Administrator، توسط یک حساب domain Admin وارد شده و cmd را باز کرده و به ترتیب وارد می کنیم:

```
Ntdsutil
set dsrm password
reset password on server null
```

- **حال یک رمز عبور وارد می کنیم.**
- **جهت تایید، دوباره آن را وارد می کنیم.**
- **پس از دریافت تایید موفقیت آمیز بودن آن، حرف q را وارد می کنیم.**
- **و دوباره حرف q را وارد می کنیم و تمام.**

نکته: تنها درصورتی که Server را در حالت Safe mode تنظیم و restart کرده باشیم، می توانیم توسط local administrator و این رمزعبور dsrm وارد سیستم شویم، و در حالت عادی، خطای اشتباه بودن رمزعبور یا شناسه کاربری می دهد.

Types of Windows Versions :

OEM :

- نسخه ی OEM (**O**riginal **E**quipment **M**anufacturer) نسخه ای از سیستم عامل های مایکروسافت می باشد که از پیش بر روی سخت افزار نصب می شود، که به اصطلاح به آن ویندوز ارجینال گفته می شود.
- به همین دلیل در هنگام خرید لپ تاپ، DVD ویندوز دریافت نمی کنیم. چون Serial Number آن از قبل روی آن تنظیم شده و بطور دائمی و همیشگی، ثبت است.
- مهمترین مشکلی که در رابطه با محصولات OEM وجود دارد این است که شما نمی توانید اقدام به نصب مجدد آن کنید، و فقط همان یکبار که از قبل نصب شده است، امکانپذیر است! تنها قادر به Update خواهیم بود.
- اما در حالتی دیگر، شرکت ماکروسافت، اقدام به فروش ویندوزهای OEM بر روی DVD می کند و شرکت ها یا حتی افراد معمولی هم قادر به خرید آن خواهند بود. و به محض اینکه آن را روی سیستم نصب کنید، درست مثل یک ویندوز ارجینال که از اول روی سخت افزار نصب شده بوده است، خواهد بود. و همان مزایا و عیب عدم نصب مجدد، را نیز خواهد داشت.

Retail :

- ویندوز Retail، پس از نصب روی سیستم، شماره سریالش را به شماره ی منحصربفرد motherboard که UUID نام دارد، اختصاص می دهد، به همین جهت تنها در شرایطی که مادربورد سیستم را تعویض کنید، آن ویندوز، بی اعتبار خواهد بود. هر ویندوز فقط روی یک سیستم جواب می دهد، و تعویض مادربورد به معنای تعویض سیستم است.

- لایسنس های Retail به صورت نامحدود اعتبار دارند و هیچ گونه محدودیتی برای زمان، تعداد دفعات فعالسازی بر روی یک سخت افزار و آپدیت ندارند.

Volume Licensing :

- این نسخه از ویندوز، با نام های دیگری چون VL و VLK (Volume Licence Key) هم شناخته شده و به عنوان نسخه ی شرکتی یا سازمانی مایکروسافت عرضه می شود.
- فرض کنید که سازمانی دارای صد ها Client است. منطقی نیست که برای هرکدام از این چند صد Client، یک License ویندوز خریداری کنیم. در چنین شرایطی مایکروسافت محصولات Volume License را ارائه نموده که با خرید آن، به میزان هزینه ای که پرداخت می کنیم، مجوز نصب دریافت می کنیم.
- این تعداد مجوز، از حداقل 5 عدد تا نامحدود می باشد و برخی از این محصولات، احتیاجی به فعال سازی ندارند.

- Volume Licensing چند Mode دارد:

❖ **MAK (Multiple Activation Keys) :**

- برای شبکه ی با کمتر از 50 کلاینت استفاده می شود.
- خودش دو Mode دارد:
  - **Independent (مستقل):**
    - مشابه با Retail است و برای هریک از Client ها یک کلید MAK دریافت می کنیم.
    - هریک از Client ها برای فعالسازی توسط کلید MAK باید از طریق اینترنت به سایت Microsoft متصل شوند.
  - **Proxy Activation :**
    - نیاز به یک Proxy Server خواهیم داشت که خودش به اینترنت و سایت Microsoft متصل خواهد شد.

❖ **KMS (Key Management Service) :**

- برای شبکه های بزرگ (بالای Client 50) کاربرد دارد.
- شامل یک KMS Server است که دارای یک License به نام KMS host key است که برای فعالسازی، به سایت Microsoft متصل می شود.
- KMS Server یک Server است که Role مربوطه را به بر روی آن نصب و پورت 1688 را بر روی Firewall آن باز می کنیم.
- Client ها را طوری تنظیم می کنیم که از طریق پورت 1688 درخواست های فعالسازی را به KMS server ارسال کنند.
- Client ها از طریق سرویس VLMCS آدرس KMS Server را پیدا می کنند.
- Client ها نیازی به دسترسی به اینترنت جهت فعالسازی License ندارند، دسترسی به KMS Server کافی ست.
- KMS server هر ۱۸۰ روز اقدام به فعالسازی مجدد می کند، و هر Client هر ۷ روز اقدام به فعالسازی مجدد می کند.
- Client ها هر 120 دقیقه یکبار، سرویس VLMCS را چک می کنند.
- در صورتی که KMS Server خراب شود، چیزی برای Restore کردن وجود ندارد. فقط یک Server جدید نصب کرده، و Role مربوط به KMS را نصب کرده و KMS host key را وارد کرده و اقدام به فعال سازی می کنیم.
- KMS Server می تواند هزاران Client را سرویس دهی کند.

❖ **ADBA (Active Directory Based Activation) :**

- مشابه KMS است، اما نیازی به Role مربوط به KMS نیست، چرا که تنظیمات را درون Active Directory انجام می دهیم.
- در این حالت، تا زمانی که Client ها به شبکه ی Domain متصل هستند، Active بوده و وقتی قطع می شوند، inactive!

❖ **AVMA (Automatic Virtual Machine Activation) :**

- سرویس AVMA را هم بر روی VM های موردنظر و هم بر روی سیستم Host، نصب و راه اندازی می کنیم.
- سرویس AVMA در HOST با سایت Microsoft ارتباط برقرار کرده و فعال شده و VM ها را نیز فعال می کند.
- AVMA برای سیستم HOST، فقط نسخه ی Data Center را پشتیبانی می کند.

KMS - Volume Licensing :

نکته: می توان خود Active Directory Server را به عنوان KMS Server در نظر گرفت، و یا می تواند یک Server جدا باشد.

نکته: راه اندازی یک KMS Server مستلزم وجود حداقل 25 کلاینت و یا حداقل 5 سرور در شبکه می باشد، که در غیر اینصورت با خطای 0xC004F038 مواجه خواهیم شد.

1. **درون سیستم KMS Server و در cmd، به سیستم DNS Server دستور NSLOOKUP را تست می کنیم که باید نتیجه ی مشخص و صحیحی بدهد.**

2. **Role مربوط به Volume Activation Services را نصب می کنیم.**
   - پس وارد Manage > Add Roles and Features شده و آن را نصب می کنیم.

3. **روی آیکون Notifications کلیک کرده و وارد تنظیمات Volume Activation Tools می شویم.**
   - **می توانیم ADBA را انتخاب کرده و نصب را تا انتها برویم و یا KMS را انتخاب و در Browse سیستم KMS Server یا حتی خود سیستم DC اصلی را انتخاب کرده و next.**
   - **KMS Host Key را وارد کرده و commit.**

نکته: اگر یک License Key مجاز نداریم، می توانیم به جای سه مرحله ی بالا، فایل License Crack را دانلود و نصب کنیم!

نکته: تا اینجا باید خود ویندوزی که قرار است KMS Server باشد، در وضعیت Activated باشد.

نکته: اگر وارد کنسول Services شویم، باید سرویس KMS Server Service در حالت Running باشد.

4. **در کنسول DNS تنظیمات KMS Server را انجام می دهیم.** (تا Client ها KMS Server را شناسایی کنند)
   - **بر روی Forward Lookup Zone اصلی شبکه، کلیک راست و Other new Records را می زنیم.**
   - **در کادر بالا، Server Location (SRV) را انتخاب کرده و Create Record را می زنیم.**
   - **برای Service درج می کنیم: _VLMCS و برای Protocol درج می کنیم: _TCP**
   - **برای Port Number درج می کنیم: 1688**
   - **برای Host offering this service آدرس سروری که KMS Server خواهد بود را کرده و OK و Done!**

5. **تنظیمات Firewall را در KMS Server انجام می دهیم.**
   - **وارد WF.msc می شویم.**
     - **Inbound Rule را و سپس New Rule را می زنیم.**
     - **Port را انتخاب کرده و نوع آن را TCP انتخاب کرده و برای Specific local Port مقدار 1688 را درج می کنیم.**
     - **Allow The Connection را زده و هرسه Profile را انتخاب و یک Name درج کرده و تمام!**
     - **دقیقا این کار را برای Outbound Rule انجام می دهیم.**

6. **Client را چک می کنیم.**
   - **در ابتدا باید هریک از client های عضو Domain، بتواند Record ای که برای SRV ساختیم را ببینند.**

   پس در Client موردنظر، وارد cmd شده و دستور زیر را وارد می کنیم و باید نام و آدرس KMS Server و پورت 1688 را بدهد:

nslookup -type=srv _vlmcs._tcp

   - **برای اینکه مطمئن باشیم که Client به پورت 1688 در KMS Server متصل است، در سیستم Client، دستور زیر را در PowerShell وارد می کنیم و باید برای گزینه ی TcpTestSucceeded مقدار True را بدهد:**

```
Test-NetConnection -ComputerName ifm.payamavar.local -Port 1688
```

   - **سپس برای مشاهده ی مشخصات Activated Key ، در cmd مربوط به Client درج می کنیم:** slmgr /dlv

- در وهله ی اول، اگر در مقابل گزینه ی **Partial Product**، مقدار **8XDDG** و برای گزینه ی **Product Key Channel** مقدار **GVLK** وجود نداشت (معمولاً **Retail** درج شده است) باید این مقدار را تغییر دهیم.

GVLK (**Generic Volume License Key**) یک کلید عمومی است که **Public KMS Client Setup Key** هم گفته می شود.
GVLK برای هر نسخه از سیستم عامل های **Microsoft**، یکتا و ثابت می باشد که برای عضویت به یک سیستم فعالسازی ویندوز، به آن نیاز می باشد.
برای تغییر این کلید در هر **Client**، با دسترسی **Admin**، وارد **cmd** آن سیستم شده و یا از دستور زیر و **Key** مربوط به ویندوز موردنظر از لیست زیرین، و یا استفاده از دستور **sconfig** و انتخاب گزینه ی **Windows Activation** آن را **OK** کرده و **Restart** می کنیم:

slmgr.vbs /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

WMDGN-G9PQG-XVVXX-R3X43-63DFG	**Windows Server 2019 Datacenter**
N69G4-B89J2-4G8F4-WWYCC-J464C	**Windows Server 2019 Standard**
WVDHN-86M7X-466P6-VHXV7-YY726	**Windows Server 2019 Essentials**
M7XTQ-FN8P6-TTKYV-9D4CC-J462D	**Windows 10 Enterprise LTSC 2019**
92NFX-8DJQP-P6BBQ-THF9C-7CG2H	**Windows 10 Enterprise N LTSC 2019**
CB7KF-BWN84-R7R2Y-793K2-8XDDG	**Windows Server 2016 Datacenter**
WC2BQ-8NRM3-FDDYY-2BFGV-KHKQY	**Windows Server 2016 Standard**
JCKRF-N37P4-C2D82-9YXRT-4M63B	**Windows Server 2016 Essentials**
W269N-WFGWX-YVC9B-4J6C9-T83GX	**Windows 10 Professional**
MH37W-N47XK-V7XM9-C7227-GCQG9	**Windows 10 Professional N**
NPPR9-FWDCX-D2C8J-H872K-2YT43	**Windows 10 Enterprise**
DPH2V-TTNVB-4X9Q3-TJR4H-KHJW4	**Windows 10 Enterprise N**
NW6C2-QMPVW-D7KKK-3GKT6-VCFB2	**Windows 10 Education**
2WH4N-8QGBV-H22JP-CT43Q-MDWWJ	**Windows 10 Education N**
WNMTR-4C88C-JK8YV-HQ7T2-76DF9	**Windows 10 Enterprise 2015 LTSB**
2F77B-TNFGY-69QQF-B8YKP-D69TJ	**Windows 10 Enterprise 2015 LTSB N**
DCPHK-NFMTC-H88MJ-PFHPY-QJ4BJ	**Windows 10 Enterprise 2016 LTSB**
QFFDN-GRT3P-VKWWX-X7T3R-8B639	**Windows 10 Enterprise 2016 LTSB N**
D2N9P-3P6X9-2R39C-7RTCD-MDVJX	**Windows Server 2012 R2 Standard**
W3GGN-FT8W3-Y4M27-J84CP-Q3VJ9	**Windows Server 2012 R2 Datacenter**
KNC87-3J2TX-XB4WP-VCPJV-M4FWM	**Windows Server 2012 R2 Essentials**
GCRJD-8NW9H-F2CDX-CCM8D-9D6T9	**Windows 8.1 Professional**
HMCNV-VVBFX-7HMBH-CTY9B-B4FXY	**Windows 8.1 Professional N**
MHF9N-XY6XB-WVXMC-BTDCT-MKKG7	**Windows 8.1 Enterprise**
TT4HM-HN7YT-62K67-RGRQJ-JFFXW	**Windows 8.1 Enterprise N**
BN3D2-R7TKB-3YPBD-8DRP2-27GG4	**Windows Server 2012 Core**
8N2M2-HWPGY-7PGT9-HGDD8-GVGGY	**Windows Server 2012 Core N**
2WN2H-YGCQR-KFX6K-CD6TF-84YXQ	**Windows Server 2012 Core Single Language**
4K36P-JN4VD-GDC6V-KDT89-DYFKP	**Windows Server 2012 Core Country Specific**
XC9B7-NBPP2-83J2H-RHMBY-92BT4	**Windows Server 2012 Server Standard**
XC9B7-NBPP2-83J2H-RHMBY-92BT4	**Windows Server 2012 Standard Core**
HM7DN-YVMH3-46JC3-XYTG7-CYQJJ	**Windows Server 2012 MultiPoint Standard**
XNH6W-2V9GX-RGJ4K-Y8X6F-QGJ2G	**Windows Server 2012 MultiPoint Premium**
48HP8-DN98B-MYWDG-T2DCC-8W83P	**Windows Server 2012 Datacenter**
48HP8-DN98B-MYWDG-T2DCC-8W83P	**Windows Server 2012 Datacenter Core**
NG4HW-VH26C-733KW-K6F98-J8CK4	**Windows 8 Professional**
XCVCF-2NXM9-723PB-MHCB7-2RYQQ	**Windows 8 Professional N**
32JNW-9KQ84-P47T8-D8GGY-CWCK7	**Windows 8 Enterprise**
JMNMF-RHW7P-DMY6X-RF3DR-X2BQT	**Windows 8 Enterprise N**
FKJQ8-TMCVP-FRMR7-4WR42-3JCD7	**Windows Server 2008 R2 HPC Edition**
74YFP-3QFB3-KQT8W-PMXWJ-7M648	**Windows Server 2008 R2 Datacenter**
489J6-VHDMP-X63PK-3K798-CPX3Y	**Windows Server 2008 R2 Enterprise**
GT63C-RJFQ3-4GMB6-BRFB9-CB83V	**Windows Server 2008 R2 for Itanium-Based Systems**
YC6KT-GKW9T-YTKYR-T4X34-R7VHC	**Windows Server 2008 R2 Standard**
6TPJF-RBVHG-WBW2R-86QPH-6RTM4	**Windows Web Server 2008 R2**
7M67G-PC374-GR742-YH8V4-TCBY3	**Windows Server 2008 Datacenter**
22XQ2-VRXRG-P8D42-K34TD-G3QQC	**Windows Server 2008 Datacenter without Hyper-V**
4DWFP-JF3DJ-B7DTH-78FJB-PDRHK	**Windows Server 2008 for Itanium-Based Systems**
YQGMW-MPWTJ-34KDK-48M3W-X4Q6V	**Windows Server 2008 Enterprise**
39BXF-X8Q23-P2WWT-38T2F-G3FPG	**Windows Server 2008 Enterprise without Hyper-V**
TM24T-X9RMF-VWXK6-X8JC9-BFGM2	**Windows Server 2008 Standard**
W7VD6-7JFBR-RX26B-YKQ3Y-6FFFJ	**Windows Server 2008 Standard without Hyper-V**
WYR28-R7TFJ-3X2YQ-YCY4H-M249D	**Windows Web Server 2008**
FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4	**Windows 7 Professional**
MRPKT-YTG23-K7D7T-X2JMM-QY7MG	**Windows 7 Professional**
PXH-7Y6KF-2VJC9-XBBR8-HVTHH۳۳	**Windows 7 Enterprise**
YDRBP-3D83W-TY26F-D46B2-XCKRJ	**Windows 7 Enterprise N**
C29WB-22CC8-VJ326-GHFJW-H9DH4	**Windows 7 Enterprise E**
YFKBB-PQJJV-G996G-VWGXY-2V3X8	**Windows Vista Business**
HMBQG-8H2RH-C77VX-27R82-VMQBT	**Windows Vista Business N**

- دوباره برای اطمینان از برقراری ارتباط با **KMS Server** از دستور **slmgr /dlv** استفاده می کنیم.
- اگر در مقابل گزینه های **KMS** مشخصات **KMS Server** وجود نداشت، یعنی متصل نشده است، پس در **cmd** این **Client**، دستور زیر را وارد می کنیم:

slmgr /skms نام یا آدرس سرور:1688

- **Client** باید دوباره **Restart** شده و دوباره ارتباط را توسط دستور **slmgr /dlv** چک کنیم.

Firewall :

بطورکلی **Firewall** ها دو دسته اند:

- **Personal Firewall** : تنها امنیت یک سیستم را تامین می کند.
- **Network Firewall** : امنیت یک شبکه را تامین می کند.

Inbound Security: کنترل دسترسی ها از خارج به داخل سیستم، از طریق پورت ها و نرم افزارها.
Outbound Security: کنترل دسترسی ها از داخل سیستم به خارج، از طریق پورت ها و نرم افزارها.

Network Firewall ها به دو شکل قابل راه اندازی هستند:

- در هسته ی شبکه، پیکربندی می شوند.
- در لبه ی شبکه، پیکربندی شوند: بین LAN و WAN .

Windows Firewall :

برای کنترل دسترسی یک **Port** یا یک **Software** در برابر شبکه های خارجی، یا به آدرس زیر می رویم یا در**Run** می نویسیم: **wf.msc**

Control Panel > Firewall > Advanced Setting

Inbound Rules: مربوط به ترافیکی است که از خارج وارد سیست می شود.
پس در اینجا برای کنترل دسترسی ها از خارج به داخل سیستم، از طریق پورت ها و نرم افزارها، قوانینی را تعریف می کنیم.

Outbound Rules: مربوط به ترافیکی است که از داخل سیستم قصد خروج از سیستم را دارد.
پس در اینجا برای کنترل دسترسی ها از داخل سیستم به خارج، از طریق پورت ها و نرم افزارها، قوانینی را تعریف می کنیم.

مسدود (block) کردن دسترسی یک Software یا Port به محیط خارجی:

- وارد بخش **Outbound Rules** می شویم.
- در سمت راست، روی **New Rule** کلیک می کنیم.
- **Program** را انتخاب کرده و **Next**.
- مسیر نصب برنامه ی مورد نظر را، همراه با نام کامل فایل اجرایی آن درج کنید، و یا از طریق **Browse** به مسیری که قرار دارد رفته و فایل آن را انتخاب کنید، مثل:

C:\Program Files\Adobe\Photoshop.exe

- در پنجره ی بعد، گزینه ی **Block the Connection** را انتخاب و **Next**.
- در پنجره ی بعد، تعیین می کنید که برنامه، در چه نوع محیط شبکه ای، مسدود شود.
- و در پنجره ی بعد، یک نام و یک توضیح برای انسداد که تعریف کرده اید، تعیین می کنید.

نرم افزار **Block** شده نمی تواند چیزی را ارسال و یا درخواست و دریافت کند، اما دیگران او را می بینند و خودشان می توانند هرچیزی که می خواهند را ارسال یا دریافت کنند.

مسدود کردن دسترسی های خارجی به یک Software یا Port:

- باید یک Rule را بطورکاملاً مشابه، در قسمت Inbound Rules ایجاد کنیم.

این حالت، مثل یک ارتباط یکطرفه ی نامحسوس است!
نرم افزار Block شده می تواند هرچیز دلخواهی را ارسال و درخواست و دریافت کند، اما کسی او را نمی بیند.

- این روش برای جلوگیری از تست Update و activation نرم افزارها کاربرد دارد.

مثلاً برای خاموش کردن قابلیت Remote Desktop به سیستم جاری:

- وارد بخش Inbound Rules می شویم.
- در سمت راست، روی New Rule کلیک می کنیم.
- Port را انتخاب کرده و Next.
- TCP را انتخاب کرده و در مقابل Specific local ports شماره ی 3389 را درج می کنیم.
- Block the connection را انتخاب کرده و هرسه ی Domain و Private و Public را انتخاب می کنیم.
- یک نام درج کرده و تمام.

Troubleshootings :

- گاهی لازم است که در شبکه ی Domain ، Firewall برای یک یا چند PC غیرفعال و خاموش شود.

می توانیم یک GPO برای آن PC یا PC ها ایجاد کنیم و تنظیمات آن را باز می کنیم. پس به مسیر زیر می رویم:

Computer Configuration > Policy > Administrative Template > Network > Network Connection > Windows Firewall >

هم در پوشه ی Domain Profile و هم در پوشه ی Standard Profile، گزینه ی Windows Firewall: Protect all network Connections را باز کرده و disable می کنیم.

- فرض کنید یک شبکه برپا کرده اید و همه ی اتصالات و ارتباطات به درستی انجام گرفته باشند.

حال وقتی به یکی از سیستم ها Ping می کنید، پاسخ نمی دهد.

- یکی از اولین احتمالاتی که باعث این عدم دریافت پاسخ Ping می شود، Rule یا قاعده ای ست که سرویس ping را مسدود کرده است.

نکته: پروتکلی که سرویس Ping را فراهم می کند، ICMP (Internet Control Message Protocol) می باشد.

پس در Windows Firewall وارد بخش Inbound Rules شده و در سمت راست، روی New Rule کلیک می کنیم.
گزینه ی Predefined را انتخاب کرده و از زیرمجموعه ی آن، File and Printer Sharing را انتخاب کرده و Next.
در تب بعدی، باید دو گزینه که دارای نام یکسانی هستند را تیک زده و Next و finish:

File and Printer Sharing (Echo Request – ICMPv4 -in)
File and Printer Sharing (Echo Request – ICMPv4 -in)

- فرض کنید یک شبکه برپا کرده اید و همه ی اتصالات و ارتباطات به درستی انجام گرفته و به سادگی **Ping** نیز انجام می شود. اما وقتی به یکی از سیستم ها **Remote Desktop** می کنید، پاسخ نمی دهد.

- یکی از اولین احتمالاتی که باعث این عدم موفقیت ارتباط **Remote** می شود، **Rule** یا قاعده ای ست که سرویس **Remote Desktop** را مسدود کرده است.

پس در **Windows Firewall** وارد بخش **Inbound Rules** شده و در سمت راست، روی **New Rule** کلیک می کنیم.

گزینه ی **Predefined** را انتخاب کرده و از زیرمجموعه ی آن، **Remote Desktop** را انتخاب کرده و **Next**.

در تب بعدی، باید همه ی گزینه ها را تیک زده و **Next** و **finish**.

NTP (Network Time Protocol):

- سیستم Windows Server از سرویس W32TIME برای همزمان سازی ساعت هایش استفاده می کند.
- بصورت ایده آل، همه ی ساعت های کامپیوترهای یک Domain، زمان خودشان را با ساعت یک سیستم معتبر در شبکه، همسان سازی و هماهنگ می کنند، که این سیستم اصطلاحاً Time Server نامیده می شود.
- در یک Domain مهمترین عنصر برای احراز هویت کاربران (Authentication)، زمان است و به همین دلیل باید یک Time Server قابل اعتماد، در سرور Domain Controller خود معرفی کنید.
- سیستم عامل Windows Server بطور پیشفرض Time Server مربوط به Microsoft را به عنوان Time Source، درنظر می گیرد.

- توجه کنید که در شبکه ی Domain شما، یک DC می تواند نقش NTP Server را داشته باشد. و این DC باید نقش مربوط به PDC Emulator روی آن قرار داشته باشد. پس DC ای که دارای این نقش است، Time Server پیشفرض Domain است.

- بهترین راهکار برای سازمانی که دارای شعبات مختلفی در سطح کشور و سیستم عامل ها و تجهیزات مختلفی است که نیاز به داشتن زمان دقیق هستند، استفاده از دستگاه های Time Server است که بصورت مستقیم زمان خود را از سرورهای ماهواره ای دریافت می کنند.

- یک Time Server قابل اعتماد، Time Server ای است که تمامی Client های آن مطمئن باشند که در گذر زمان، همچنان دقیقترین زمان را دریافت می کنند.

برای اینکه NTP Client بخواهد راجع به NTP Server ها بداند و آنها را بشناسد راههای بسیاری وجود دارد:

- سرورهای NTP می توانند به صورت دستی برای شبکه معرفی و تنظیم شوند.
- از طریق تنظیمات DHCP به تمام PC ها و حتی Switch ها، Router ها و Access Point ها و سایر دستگاه ها معرفی شوند.
- NTP Server ها می توانند تنظیمات زمان و تاریخ را توسط بسته های Multicast یا Broadcast روی شبکه ارسال کنند.

فرض کنید شرکتی دارای 12 هزار کلاینت و 4 عدد DC است.

- DC1 وظیفه ی نگهداری PDC Emulator را بر عهده دارد.
- شما یک دستگاه NTP Server خریداری کرده اید که زمان را بصورت دقیق از ماهواره دریافت می کند و این دستگاه را به نام NTP1.payamavar.local به DNS معرفی کرده اید.
- با وارد کردن دستور زیر در پنجره Cmd در DC1 شما این سرور NTP را به عنوان Time Source دقیق سازمان بعنوان پیشفرض معرفی می کنید.

w32tm /config /manualpeerlist:"ntp1.ITPerfection.local" /syncfromflags:manual /reliable:yes /update

اگر قصد دارید چندین سرور NTP در مجموعه داشته باشید که در صورت بروز مشکل برای یکی از آنها، بقیه دچار مشکل نشوند، کافیست بعد از نصب دستگاه جانبی یا سرور جانبی، آدرسی که در manualpeerlist وارد می کنید را با علامت کاما از هم جدا کنید ، اگر فرض را بر این بگیریم که ما دو عدد NTP در سازمان داشته باشیم معرفی آنها به شکل زیر خواهد بود:

w32tm/config/manualpeerlist:"ntp1.ITPerfection.local,ntp2.ITPerfection.local"/syncfromflags:manual /reliable:yes /update

توصیه می شود که این دستور را نه تنها در PDC Emulator بلکه بر روی تمامی DC های مجموعه اجرا کنید و حتی اگر تعداد DC های شما در مجموعه های Forest زیاد است، آن را از طریق GPO یا Logon ScrIPt به همه DC ها اعمال کنید.

اگر در سازمان خود NTP ندارید تا جای ممکن، از NTP Server های اینترنتی استفاده نمی کنیم و IP Address های سرورهای DC را به عنوان NTP به شبکه معرفی می کنیم، اگر این موارد را به درستی رعایت کنیم، زمانیکه ساعت رسمی کشور به عقب یا جلو می رود کافیست که فقط زمان سرور PDC Emulator را یک ساعت به عقب یا به جلو بکشیم تا از بروز مشکلات جانبی جلوگیری شود.

Users, Computers, Groups :

پس از نصب AD چند گزینه ی مهم به فهرست Tools در Server Manager اضافه می شوند.
هر کاربر و هر کامپیوتر و هر گروه کاربران، دارای یک Object درون Active Directory می باشد، که دارای مشخصاتی می باشند.

هر Object در AD، علاوه بر نام و همه ی مشخصاتی که بطور دستی می توان برای آن تعریف کرد، دارای یک شماره ی یکتا به نام SID هم می باشد.
پس اگر یک User به نام ABC ایجاد کنیم و آن را حذف کنیم؛ و دوباره یک User به همان نام ABC ایجاد کنیم، به هیچ وجه آن User قبل نخواهد بود، چون دارای یک SID دیگر خواهد بود.
Object ها را در Active Directory Users and Computers ایجاد می کنیم که راه میانبر برای فراخوانی آن، این است که در Run درج کنیم:

dsa.msc

وقتی آن را باز کنید، در سمت چپ، در زیرمجموعه ی Domain ای که ساخته ایم، چند پوشه می بینیم که مهم ترین آنها:

- **Builtin** : تمام Group هایی که برای دسته بندی User ها به شکل Default در AD قرار دارند را می بینیم.
- **Computers** : کامپیوترهای متصل به شبکه ی Domain را می بینیم.
- **Domain Controllers** : سیستم یا سیستم هایی که به عنوان DC در شبکه عضو هستند را می بینیم، که آنها را با PC Name ای که دارند، نشان می دهد، که در حقیقت، اولین گزینه، همیشه خود سیستم در حال اجراست!
- **Users** : حساب های کاربری که از قبل توسط خود سیستم، در Domain ایجاد شده اند را می بینید.

در پوشه ی Users می توان به سادگی User های زیادی ساخت، که پس از ایجاد آنها با دابل کلیک به تنظیمات آنها دسترسی داشت.

نکته:

برای مدیریت بهینه تر و قوی تر User ها و Group ها، می توان از کنسول Active Directory Administrative Center هم استفاده کرد.

Work on Users :

New-AdUser :

وقتی تعداد User های مورد نظر برای ایجاد، خیلی زیاد باشند، ایجاد آنها در Powershell راحت تر و سریع تر خواهد بود.
اول باید بدانیم که یک User، شش ویژگی منحصر به فرد دارد که در تعریف آن، الزامی می باشند:

Name :

بصورت مقابل بکار می رود: **-Name**

First Name :

بصورت مقابل بکار می رود: **-GivenName**

Last Name:

بصورت مقابل بکار می رود: **-SurName**

Account Name : نام Account است که با آن Login می کنیم.

بصورت مقابل بکار می رود: **-SamAccountName**

Prinsipal Name : نام دومینیِ User است، که علاوه بر SamAccountName، شامل Root Domain Name نیز است.

بصورت مقابل بکار می رود: **-UserPrincipalName**

Password : رمز عبور

بصورت مقابل بکار می رود: **-AccountPassword(ConvertTo-SecureString -AsPlainText "XXXX" -force)**

در حقیقت می توان گزینه ی UserPrincipalName و AccountPassword را تعیین نکرد، اما آنگاه:

- ❖ User ایجاد شده، هنوز عضو هیچ Domain ای نیست و باید بعداً بصورت دستی در Properties آن، نام Domain را انتخاب کرد، که اگر تعداد User های ایجاد شده زیاد باشد، دردسر اضافه ست!
- ❖ برای فعال سازیِ User، باید دستور زیر را هم در انتها اضافه کرد:

-Enabled $true

- ❖ اما چون پسوردی برای آن تعریف نکرده ایم، نمی تواند فعال باشد، مگر اینکه خط زیر را هم در ادامه ی دستورات درج کنیم:

-PasswordNotRequired $true

مثلاً تعریف یک حساب کاربری، در دامینی به نام **payamavar.local**:

```
New-ADUser -name "A B"-Givenname A -Surname B -SamAccountname AB -UserPrincipalName AB@payamavar.local
-AccountPassword(ConvertTo-SecureString -AsPlainText "XXXX" -force) -Enabled $true
```

البته برای ایجاد راحت تر و سریع تر یک User در PowerShell می توان، در سمت راست PowerShell، یعنی در تب Commands، دستور New-AdUser را جستجو و پیدا کرد و در تب پایین، همه ی مشخصات دلخواه را وارد و Run کرد.

فقط باید دقت کرد که :

- ➢ برای تعریف **Password** ایراد می گیرد، پس می توان بعداً آن را تعیین کرد!
- ➢ برای نام **Country** معمولاً ایراد می گیرد، پس ضروری هم نیست!
- ➢ برای گزینه هایی که باید فعال یا غیرفعال باشند، **$true** و یا **$false** درج می کنیم.
- ➢ گزینه هایی که به سادگی می توان وارد کرد:
  - **Name** : نام کامل
  - **City**
  - **Company**
  - **Department**
  - **Display Name**
  - **Given Name**
  - **Mobile Phone**
  - تیک گزینه ی **Pass Thru** را فعال می کنیم.
  - **Postal Code**
  - **SamAccountName**
  - **SurName**
  - **Title** : همان **Job Title** است.
  - **UserPrincipalName**

Distinguished Name :

هر آبجکت درون **Active Directory** دارای یک آدرس **Distinguished Name** (یا DN) است، که این **DN** برای هر **Object**، منحصر به فرد است، یعنی هیچ دو آبجکتی دارای **DN** یکسان نخواهند بود.

DN دارای اجزای زیر است:

- ❖ **DC=** : نشان دهنده ی نام **Domain** است (Domain Component).
  نام Domain ممکن است چند بخشی باشد.مثل IT.Local.ir که DC در اینجا برابر می شود با "DC=IT, DC=Local, DC=ir"
- ❖ **OU=** : نشان دهنده ی نام Organizational Unit است.
  اگر یک OU با نام Test، در Domain بالا داشته باشیم، آدرسش برابر است با "OU=Test, DC=IT, DC=Local, DC=ir"
- ❖ **CN=** : نشان دهنده ی نام هر **Object** درون **AD** است (Common Name)، مثل **User** ها، **Computer** ها، **Group** ها و ...
  اگر در Domain بالا یک User به نام Saeed درون OU به نام Test داشته باشیم، آدرس DN آن برابر می شود با:
  "CN=Saeed, OU=Test, DC=IT, DC=Local, DC=ir"

: Get-AdUser

برای مشاهده ی User های تعریف شده و یا دریافت اطلاعات در مورد User ها، از دستور Get-AdUser در سمت راست پنجره ی PowerShell ، در تب Commands استفاده می شود. بعد از پیدا کردن و انتخاب آن، در تب پایینِ آن، show details را انتخاب می کنیم. وارد تب Identity شده و نام هریک از User های دلخواه را می توان کرد، تا مشخصات آن ظاهر شوند.

❖ مشاهده ی مشخصات یک User :

```
Get-ADUser -Identity Payam1
```

❖ برای مشاهده ی همه ی User های عضو شبکه و یا User ای که بخشی از نام آن را می دانیم:

```
Get-ADUser -Filter *
Get-ADUser -Filter "name -like '*payam*'"
```

❖ گاهی نام یک User را داریم، و فقط یک سری از مشخصات آن را می خواهیم:

```
Get-ADUser -Identity Payam1 -Properties "SamAccountName","LastLogonDate","UserPrincipalName"
```

❖ دریافت تاریخ ایجاد یک User :

```
Get-ADUser -Identity payam1 -Property whenCreated | FT Name, whenCreated -Autosize
Get-ADUser -Filter 'Name -like "*rebecca*"' -Property whenCreated
```

❖ مشاهده ی User هایی که طی 30 روز اخیر ایجاد شده اند:

```
$D1=(Get-Date).AddDays(-30)
Get-ADUser -Filter * -Property whenCreated | Where {$_.whenCreated -gt $D1} | FT Name,
whenCreated -Autosize
```

❖ دریافت همه ی User های فعال، همراه با آدرس DistinguishedName شان:

```
Get-ADUser -Filter 'enabled -eq "true"' | FT Name,distinguishedname
```

❖ دریافت همه ی User های غیرفعال، همراه با آدرس distinguishedname شان:

```
Get-ADUser -Filter * | Where-Object {$_.Enabled -like “false”} | FT Name,Enabled,distinguishedname
```

❖ دریافت مشخصات یک کامپیوتر که، بخشی از نام آن را می دانیم:

```
Get-ADObject -Filter 'Name -like "*NB01*"'
```

❖ دریافت مشخصات یک کامپیوتر که می دانیم در یک OU خاص قرار دارد و بخشی از نام آن را می دانیم:

```
Get-ADObject -Filter 'Name -like "*NB01*"' -SearchBase "DC=dc1,DC=payamavar,DC=local"
```

❖ دریافت نام کامل، User name، تاریخ ایجاد، آخرین تاریخ login به شبکه، آدرس DistinguishedName و وضعیت فعال/غیرفعال بودن یک User، که بخشی از نامش را می دانیم:

```
Get-ADUser -Filter 'Name -like "*Rana*"' -Properties “LastLogonDate","whenCreated",
"SamAccountName","distinguishedname"| select name, SamAccountName, whenCreated, LastLogonDate,
enabled, distinguishedname | Format-List
```

❖ یک Account را فعال می کنیم (توسط یکی از دستورهای زیر):

```
Get-ADUser USERNAME | Enable-ADAccount
Enable-ADAccount -Identity USERNAME
```

❖ یک Account را غیرفعال می کنیم:

```
Disable-ADAccount -Identity USERNAME
```

❖ تمام user هایی که درون یک OU هستند را disable می کنیم:

```
Get-ADUser -Filter "Name -like "*" -SearchBase "OU=TempUsers,DC=Test, DC=Local" | Disable-ADAccount
```

❖ در شبکه های بزرگ، که دارای Child domain هستند، پیدا کردن زمان آخرین Login توسط دستورهای معمولی یا تب Attribute editor در Active directory دقیق نخواهد بود! پس از دستور زیر استفاده می کنیم:

```
$username = "USERNAME"
[datetime]::FromFileTime((Get-ADDomainController -Filter * | foreach {Get-ADUser $username -
Properties LastLogon -Server $_.Name | select LastLogon} | Measure-Object -Property LastLogon
-Maximum).Maximum)
```

❖ برای پیدا کردن مشخصات User های فعال در یک OU خاص (و همچنین OU های زیرمجموعه ی آن):

```
$ou="OU=RLS,DC=berlin,DC=rosa,DC=de"
Get-ADUser -Filter {Enabled -eq $true} -SearchBase $OU | select Name, SamAccountName,
DistinguishedName, LastLogonDate | Format-Table
```

❖ برای پیدا کردن User های فعالی که طی 30 روز گذشته، در شبکه login نکرده اند، در یک OU خاص (و OU های زیرمجموعه ی آن):

```
$ou="OU=RLS,DC=berlin,DC=rosa,DC=de"
Get-ADUser -Filter {Enabled -eq $true} -SearchBase $ou -Properties
Name,SamAccountName,LastLogonDate,LastLogon | select SamAccountName,LastLogonDate | Where
{($_.LastLogonDate -lt (Get-Date).AddDays(-30)) -and ($_.LastLogonDate -ne $NULL)} | Sort |
Select SamAccountName,LastLogonDate,distinguishedName
```

: Set-AdUser

برای ایجاد تغییر در User های تعریف شده در AD، از این دستور استفاده می شود.

پس در تب Commands این دستور را پیدا کرده و در تب Identity Add، محتویات آن را تغییر داده و Run !

مثال: فرض کنید بخواهیم:

- قسمت Description یک Account را بطورکامل تغییر دهیم:

```
Set-ADUser -Identity Payam.avar -Description "This is test User."
```

- به ابتدا یا انتهای Description یک Account ، مقداری را اضافه کنیم:

```
$User = Get-ADUser -Identity payam.avar -Properties Description
$USC=$User.Description
Set-ADUser -Identity Payam.avar -Description "This is a $USC"
```

مثال:

می دانیم که برای هر User Account در تب Organisation تنظیمات آن، سه مشخصه ی کاربردی وجود دارند:

- Job Title که عنوان یا پست شغلی را مشخص می کند.
- Department، که بخشی از سازمان که کاربر در آنجا کار می کند را مشخص می کند.
- Company، که نام کامل سازمان یا شرکت را نشان می دهد.

فرض کنید بخواهیم، یکی از آنها را برای یک User تغییر دهیم:

```
Set-ADUser -Identity Payam.avar -Title "Office director"
Set-ADUser -Identity Payam.avar -Department "IT"
Set-ADUser -Identity Payam.avar -Company "RLS"
```

درحقیقت گاهی لازم است که بخش های دیگری از یک یا یک سری Account را تغییر دهیم، که برای آن بخش ها، دستورات خاص خودشان را باید استفاده کرد. مثلن:

- جهت تغییر تاریخ انقضای یک Account:

```
Set-ADAccountExpiration -Identity Payam.avar -DateTime "01/01/2024"
```

- جهت تمدید تاریخ انقضای یک Account، تا 45 روز بعد از تاریخ کنونی آن:

```
Set-ADAccountExpiration -Identity payam.avar -TimeSpan 45.0:0
```

- جهت تغییر تاریخ انقضای Account هایی که در AD، عضو یک Group هستند:

```
Get-ADGroupMember -Identity Test_Group | where {$_.objectClass -eq "user"} |
Set-ADAccountExpiration -DateTime "01/01/2024"
```

- جهت تغییر تاریخ انقضای Account هایی که تاریخ انقضای کنونی آنها، تا 30 روز آینده است:

```
$ou = "OU=RLS,DC=berlin,DC=rosa,DC=de"
$User = Get-ADUser -Filter {Enabled -eq $true} -SearchBase $ou -Properties SamAccountName,
AccountExpirationDate, office | where {($_.AccountExpirationDate -notlike '') -and
($_.AccountExpirationDate -lt (Get-Date).AddDays(30))}
foreach ($U in $User){
Set-ADAccountExpiration -Identity $U -DateTime "01/01/2024"
}
```

: Remove-AdUser

برای ایجاد حذف هریک از این User ها، در AD، از این دستور استفاده می شود.

Remove-ADUser نام اکانت

توسط دستور زیر، همه ی حساب های Disabled ، حذف خواهند شد:

```
Get-ADUser -Filter 'enabled -eq "false"' | Remove-ADUser
```

: Search-ADAccount

برای جستجوی User ها بکار می رود. مثال:

- برای پیدا کردن همه ی Object هایی که غیرفعال هستند، همراه با آخرین ورودشان به شبکه:

```
Search-ADAccount -AccountDisabled | select Name,LastLogonDate,Enabled
```

اگر بخواهیم فقط میان کامپیوترها یا فقط میان User ها بگردد، از یکی از سوییچ های ComputerOnly- یا UserOnly- استفاده می کنیم.

- برای پیدا کردن فقط Object های کامپیوترهایی که غیرفعال هستند:

```
Search-ADAccount -AccountDisabled -ComputerOnly | select Name, LastLogonDate, Enabled
```

- برای پیدا کردن Object هایی که طی دو روز اخیر، روشن نشده اند (متصل نشده اند):

```
Search-ADAccount -AccountInactive -Timespan 2
```

- برای پیدا کردن User Account های باطل شده:

```
Search-ADAccount -AccountExpired -UsersOnly | select Name, LastLogonDate, Enabled
```

نکته: اگر تنها بخواهیم تعداد این Object ها را بدانیم، کافیست در انتهای دستور، یک Pipe درج کرده و: Measure-Object

- برای پیدا کردن Object های در حال ابطال:

```
Search-ADAccount -AccountExpiring
```

- برای پیدا کردن Object هایی که از X روز گذشته تا الان، log in نکرده اند:

```
Search-ADAccount -AccountInactive -Timespan X
```

```
dsquery user "ou=Test,dc=IT,dc=Local" -inactive 2
dsquery computer "ou=Test,dc=IT,dc=Local" -inactive 2
```

: Change the Password

Set-ADAccountPassword payam1 -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "123456" -Force)	**In PowerShell**
net user payam1 654123	**In CMD**

Attribute Editor :

یکی از تب های **Properties** هریک از **Object** های موجود در **Active Directory** می باشد که شامل مقادیر و مشخصات زیادی می باشد. توسط دکمه ی **Filter** در پایین می توان نوع نمایش این مقادیر را تغییر داد.

- ✓ برای مشاهده ی **Distinguished Name مربوط به یک Object**، گزینه ی **distinguished name** را در این تب انتخاب کرده و **view** را می زنیم.
- ✓ **زمان و ساعت آخرین اتصال به شبکه**: گزینه ی **lastLogonTimestamp**
- ✓ گاهی لازم است که یک سری **Account** های خاصی که در **AD** ایجاد می کنیم، در سیستم **Email** شبکه، (مثل **Outlook**) در لیست مخاطبین (**Address Book**) ظاهر نشوند، پس وارد تنظیمات آن **User** ها در **AD** شده و در تب **Attribute Editor**، مشخصات گزینه ی **ShowInAddressBook** را کاملن پاک می کنیم.

CSVDE (Comma Separated Value Data Exchange) :

فرض کنید قرار باشد، سیستم **Domain Controller** یک شبکه ی بزرگ را که شامل بیش از **100** کاربر است، تغییر دهید، در نتیجه باید در **Domain Controller** جدید، همه ی **User** ها و محتویات **Active Directory** را نیز داشته باشید؛ اما چگونه؟!

ما می توانیم توسط ابزارِ دستوری **CSVDE** تمام **Object** ها را درون یک فایل، **Export** کنیم و در **DC** جدید آن فایل را **Import** کنیم.
نوع **Object** را توسط **objectClass** مشخص می کنیم که شامل مقادیر زیر می باشد:

- ❖ **Person** برای **User** ها
- ❖ **Group** برای **Group** ها
- ❖ **Container** برای **Container** ها
- ❖ **organizationalUnit** برای **Organizational Unit** ها
- ❖ **Computer** برای **Computer** ها
- ❖ و ...

- دستور زیر، همه ی **Object** های **Active Directory** را درون یک فایل **csv.** به نام **AD1** و در درایو **C** ذخیره می کند:

csvde -f c:\AD1.csv

- دستور زیر، همه ی **User** های موجود در **AD** را درون یک فایل **csv.** به نام **AD1** و در درایو **C** ذخیره می کند:

csvde -f c:\AD1.csv -r objectClass=Person

- دستور زیر، سه مشخصه از همه ی **OU** های موجود در **AD** را درون یک فایل **csv.** به نام **AD1** و در درایو **C** ذخیره می کند:

csvde -f c:\AD1.csv -r objectClass=organizationalUnit -l "DN, name, distinguishedName"

توسط سوییچ **f-** : یک نام برای فایل ذخیره تعیین می کنیم.

توسط سوییچ **r-** : یک فیلتر جستجو، برای export ایجاد می کنیم.

توسط سوییچ **L-** : لیستی از **attribut** های نتیجه ی نهایی دستور را تهیه و پاسخ نهایی را توسط این دستور، تنظیم می کنند.

:CSVDE Export

فرض کنید در AD شبکه ی Payamavar.local یک OU داریم به نام Employee که دارای صد User است و می خواهیم از همه ی آنها Import گرفته و آنها را وارد Domain شبکه ی Avar.local و در OU به نام EMP کنیم.

وارد cmd شده و دستور زیر را درج می کنیم:

csvde -d "Distinguished Name of OU" -f X:\FileName.csv

csvde -d "OU=Employee,DC=payamavar,DC=local" -f c:\Employee.csv

پس اطلاعات همه ی User های موجود در OU کارمندان، در فایلی در درایو C ذخیره می شوند، که می توان آنرا با Excel هم باز کرد.

- همانطور که می بینیم، همه ی ستون های موجود اهمیت زیادی نخواهند داشت، می توانیم خیلی از ستون ها را حذف کنیم، اما ستون های اساسی عبارتند ا ز:

DN | objectClass | ou | distinguishedName |

Name | cn | sn | givenName | displayName |

sAMAccountName | userPrincipalName

- چون می خواهیم User ها را در Domain جدید در یک OU جدید وارد کنیم، پس لازم است که سطر دوم را کاملاً حذف کنیم.
- با توجه به اینکه Domain جدید نام متفاوتی دارد، پس وارد ابزار Find and Replace شده و سه تغییر زیر را اعمال می کنیم:

✓
  - برای Find What درج می کنیم: DC=payamavar,DC=local
  - برای Replace with درج می کنیم: DC=Avar,DC=local

✓
  - برای Find What درج می کنیم: Payamavar.local
  - برای Replace with درج می کنیم: Avar.local

✓
  - برای Find What درج می کنیم: Employee
  - برای Replace with درج می کنیم: EMP

و فایل را ذخیره کرده و به Server جدید منتقل می کنیم.

:CSVDE Import

در Server جدید، مثلا فایل Export شده را به درایو C می بریم.

وارد cmd شده و درج می کنیم:

csvde -i -f c:\ Employee.csv

حال اگر به کنسول AD Users and Computers برویم، می بینیم که OU به نام EMP ایجاد شده و User ها درون آن هستند، تنها باید آنها را Enable کرد! پس همه را انتخاب کرده و کلیک راست کرده و Enable Users را می زنیم.

Dsquery و Dsget :

دستورات **Dsquery** و **Dsget** دستورات قدرتمندی هستند که بوسیله ی آنها می توان اطلاعاتی در مورد **Object** های موجود در **Active Directory** کسب کرد.
نکته: این دستورها، فقط می توانند اطلاعات مربوط به **Object** های درون **OU** ها را بدست آورند و نه **Container** ها را!!

❖ دستور **Dsquery** لیست تمامی **Group** ها یا **User** های درون یک **OU** به نام **Test** را نشان می دهد. به عنوان مثال :
dsquery group "ou=Test,dc=IT,dc=Local"
dsquery user "ou=Test,dc=IT,dc=Local"

❖ دستور بالا تمامی **Group** ها یا **User** های موجود در **OU** و زیر شاخه های آن را به ما نشان می دهد.
اگر بخواهیم فقط گروههای درون **OU** به ما نشان داده شوند، از دستور زیر استفاده می کنیم:
dsquery group "ou=Test,dc=payamavar,dc=Local" -scope onelevel

❖ اگر بخواهیم نتیجه ی دستور بالا درون یک فایل متنی ذخیره شود:
dsquery group "ou=Test,dc=payamavar,dc=Local" > group.txt

❖ توسط دستور زیر لیستی از **User** ها و **Computer** هایی که در **4** هفته ی گذشته به **Domain** ورود نداشته اند را دریافت می کنیم:
dsquery user "dc=payamavar,dc=Local" -inactive 4
dsquery computer "dc=payamavar,dc=Local" -inactive 4

❖ مثلاً دستور زیر، لیست تمامی اعضای گروه **Domain Admin** را نشان می دهد:
dsget group "cn=Domain Admins,cn=users,dc=payamavar,dc=Local" -members

❖ توسط این دستور، می توان عضویت یک **User** در گروههای مختلف را نشان داد، در حقیقت لیست گروههایی را نشان می دهد که یک **User** مثل **Payam** در آنها عضویت دارد:
dsget user "cn=payam,ou=MyUsers,dc=payamavar,dc=Local" -memberof

:Create A bunch Of Users

فرض کنید نیاز است که در مدت خیلی کوتاهی، چند ده یا چند صد **User** را در **AD** ثبت کنیم.
می توانیم تمام مشخصات تمام کاربران را در یک فایل **Excel** خیلی ساده و روان درج کنیم، و آن فایل را در **AD** وارد کنیم.

1. همه مشخصاتِ همه ی افراد را به هرترتیب دلخواه، درون یک فایل Excel درج کرده و با پسوند csv ذخیره می کنیم.
نکته ای که مهم است این است که باید به ترتیب دلخواهی که برای مشخصات آنها در نظر گرفته ایم، توجه کنیم. مثلاً:

	A	B	C	D	E	F
1	name	sam	upn	given	sur	password
2	a1	b1	b1@payamavar.local	a1	b1	p1y1m1v1R
3	a2	b2	b2@payamavar.local	a2	b2	p1y1m1v1R
4	a3	b3	b3@payamavar.local	a3	b3	p1y1m1v1R
5	a4	b4	b4@payamavar.local	a4	b4	p1y1m1v1R
6	a5	b5	b5@payamavar.local	a5	b5	p1y1m1v1R
7	a6	b6	b6@payamavar.local	a6	b6	p1y1m1v1R

اگر روی فایل **csv** ذخیره شده، کلیک راست و **Edit** را بزنیم، با تصویر زیر مواجه می شویم:

*pop.csv - Notepad

File Edit Format View Help

```
name,sam,upn,given,sur,Password
a1,b1,b1@payamavar.local,a1,b1,p1y1m1v1R
a2,b2,b2@payamavar.local,a2,b2,p1y1m1v1R
a3,b3,b3@payamavar.local,a3,b3,p1y1m1v1R
a4,b4,b4@payamavar.local,a4,b4,p1y1m1v1R
a5,b5,b5@payamavar.local,a5,b5,p1y1m1v1R
a6,b6,b6@payamavar.local,a6,b6,p1y1m1v1R
```

2. User ها را ایجاد می کنیم.
فرض می کنیم که این فایل **csv** را در درایو **C** ذخیره کرده ایم، پس در**PowerShell ISE** دستور زیر را وارد می کنیم و **Enter** .

```
Import-Csv c:/pop.csv | ForEach-Object {New-ADUser -Name $_.name -SamAccountName $_.sam -UserPrincipalName $_.upn `
-GivenName $_.given -Surname $_.sur -Enabled $true -AccountPassword(ConvertTo-SecureString -AsPlainText $_.Password -Force)}
```

نکته: برای تعیین اینکه این **User** ها در یک **Container** یا **OU** خاص ایجاد شوند، می توان از دستور **Path-** استفاده کرد که در مقابل آن آدرس **distinguishedName** مربوط به مقصد را درون " " باید درج کرد.

```
-Path "DC=myUsers, DC=Payamavar, DC=local"
```

: Recycle Bin

این قابلیت باعث می شود تا برای restore کردن Object های حذف شده ی کنسول AD Users and Computers، نسبت به Restore کردن فایل Backup، بی نیاز شویم.

نکته: وقتی که این قابلیت را فعال می کنیم، به این سادگی ها قابل غیرفعال کردن نخواهد بود.

این سطل زباله، دقیقاً مثل سطل زباله ی خود ویندوز عمل می کند که از ویندوز سرور 2012 به بعد اضافه شده است.

برای فعال کردن آن وارد AD Administrative Center می شویم و در سمت چپ، Domain را انتخاب می کنیم و در سمت راست، Enable Recycle Bin را انتخاب می کنیم و yes!

اگر خطایی مشابه the FSMO Role ownership could not be verified بالا آمد:
باید فایل های NTDS را در کنسول AD Sites and Services یکبار Replicate کنیم.

بصورت پیشفرض آبجکت حذف شده تا 180 روز قابلیت بازیابی دارد که البته این مقدار را میتوان تغییر داد.

: Profile

اگر وارد Properties یک User شویم، در تب Profile با موارد زیر روبرو خواهیم شد.

: Profile Path

فرض کنید کاربری برای اولین بار از طریق کامپیوتر Client 52 به شبکه logon می کند.

- این کاربر فایل اکسلی به نام common.xlsx ایجاد می کند.
- برنامه ی Microsoft Excel را نیز برای خودش customize می کند.
- یک فایل jpg را نیز روی دسکتاپ قرار داده و سپس log out می کند.

فردا این کاربر، با همان Credential خودش، از طریق کامپیوتر Client 58 به شبکه logon می کند.
اما وقتی وارد می شود، روی دسکتاپش نه خبری از فایل common.xlsx است و نه از فایل jpeg!
البته اگر دوباره از طریق Client 52 وارد شود، همه چیز سر جای خودش است.
در این حالت گفته می شود که Profile او، حالت roaming ندارد؛ و باید این حالت را برای User ها ایجاد کرد.
اگر در این زمان توسط هریک از User ها در یکی از سیستم های شبکه Log in کنیم و به آدرس زیر برویم، و change Type را بزنیم، می بینیم که فقط بر روی Local قرار دارد:

```
Run > Sysdm.cpl > Advanced Tab > User Profile > Settings
```

برای راه اندازی این قابلیت، کافیست، یک پوشه را در شبکه Share کنیم و Share Permission آن را برای Everyone روی Read قرار داده و NTFS Permission آن را برای User یا User های موردنظر Full قرار دهیم و سپس آدرس UNC آن را کپی کنیم.
حال در AD Users and Computers، User های موردنظر را همزمان انتخاب کرده و وارد Properties شده و در تب Profile و نوار Profile Path، آن آدرس UNC را درج کنیم، البته همراه با عبارت ٪username٪ در انتها. (و یا فقط نام آن User را درج کنیم)

البته قابلیت Roaming profile می تواند باعث افزایش ترافیک شبکه شود، به خصوص اگر کاربران، فایل های حجیم و سنگینی را روی دسکتاپ هایشان ذخیره کنند.
پس بهتر است یا از این قابلیت استفاده نکرد و یا تذکرهای لازم به کاربران داده شود که فایل های سنگین را روی دسکتاپ شان قرار ندهند و یا از قابلیت FSRM استفاده کرد.

: Logon Script

شاید بخواهید پس از logon کردن کاربری در هریک از سیستم ها، سلسله ای از اتفاقات رخ دهد.
می توان یک batch file ساخت و درون آن، Script های نوشت که باعث اجرای آن اتفاقات شود.
این batch file را باید در Domain درون فولدر share شده ی NET-LOGON که درون فولدر معروف Sysvol قرار دارد، قرار داد.
اکنون وقتی کاربر logon می کند، اسکریپتهای این batch file یکی یکی اجرا می شوند.
البته امروزه دیگر برای انجام چنین کاری، از قابلیت های Group Policy استفاده می کنند.

: Home Folder

ممکن است در یک سازمان، دهها و صدها کامپیوتر موجود باشند.
فرض کنید که کاربران این شرکت، فایل های خود را روی کامپیوترهایشان ذخیره کنند.
در این حالت، تیم IT باید برای حفاظت این فایل ها از دسترسی های غیرمجاز و نیز از بین نرفتن این فایل ها برنامه ریزی ها کند و وقت بسیار زیادی از اعضای تیم IT نیز تلف خواهد شد.
حال اگر از Backup گیری هم استفاده شود، فضای ذخیره سازی بسیار زیاد دیگری صرف خواهد شد.

پس می توان برای همه ی کاربران، روی شبکه، یک محل مشترک برای ذخیره سازی فایل هایشان را اختصاص داد.
از نظر **Security** و **high availability**، اقدام درستی است.

کاربران موظف خواهند بود که فایل های مهم و سازمانی خود را در این محل ذخیره کنند و از طرف دیگر تیم **IT** هیچ مسوولیتی در قبال امنیت و **availability** فایل های موجود روی کامپیوترهای افراد نداشته باشد.
به **Folder** ای که جهت ذخیره سازی فایل های کاربران روی **File Server** ایجاد می شود، عموماً **Home Folder** گفته می شود.

در **Profile Path** صرفا قابلیت **roaming** برای فایل های دسکتاپ و نیز تنظیمات **Application** ها ایجاد می کنیم، اما در **Home Folder**، کاربران به انتخاب خود، فایل های حساس سازمانی را ذخیره می کنند.

برای راه اندازی آن، باید یک پوشه را به صورت مخفی در شبکه **Share** کنیم:

- پس برای **Share Name**، یک علامت **$** در انتها درج می کنیم.
- **Share Permission** را برای **Everyone** روی **Full** قرار می دهیم.
- برای **NTFS Permission** ابتدا **Disable inheritance** را زده و آن را **Convert** می کنیم.
  در پایان باید تنها گزینه های **System** و **Administrators** و **Creator Owner** باقی بمانند و **OK** و تمام!
- آدرس **UNC** این پوشه را کپی می کنیم.
- حال **User** مورد نظر را انتخاب کرده و در تب **Profile** در قسمت **Home folder** گزینه ی **Connect** را زده و یک نام درایو انتخاب کرده و آدرس **UNC** را در آنجا درج می کنیم، و نام **User** را نیز به آن اضافه می کنیم، اما اگر چند **User** را با هم انتخاب کرده باشیم، مثلاً به صورت زیر درج کرده و **Ok** می کنیم.

\\DC1\Files$\%username%

- خواهید دید که برای هریک از **User** ها، درون آن پوشه ی **Share** شده، یک پوشه به نام خودش ایجاد خواهد شد که تبدیل به یک **map drive** درون آن **User** خواهد شد.
- حال برای مدیریت فضای این **map drive** ها، می توان توسط **FSRM**، حجم آنها را کنترل کرد.

: User template

فرض کنید قصد ایجاد سناریوهای زیر را داریم:

- 12 کاربری که نباید roaming profile داشته باشند، ولی باید home folder داشته باشند.
- 10 کاربری که باید roaming profile داشته باشند، ولی نباید home folder داشته باشند.
- 20 کاربری که هم roaming profile باید داشته باشند و همhome folder.
- 5 کاربری که نه roaming profile باید داشته باشند و نه home folder.
- 17 کاربری که هیچوقت password آنها نباید expire شود.

به قطع کاری طاقتفرسا و وقتگیر خواهد بود، اما می توان آن را راحت تر کرد!
می توان یک User template ایجاد کرد، تنظیمات لازم و مورد نیاز را روی آن انجام داد و هربار از روی آن نمونه برداری کرد.

مثل ایجاد یک User عادی عمل می کنیم، با این تفاوت که در تب اول، فقط برای First name و Logon Name مثلاً یک نام یا علامت مثل # را درج می کنیم.
سپس next و Disable و بدون پسورد، تمام.
حال برای اعمال تنظیمات مورد نظر، وارد properties آن شده و اعمال می کنیم.

این کار را به تعداد حالات مورد نیاز انجام می دهیم.
و برای تمامی کاربران، روی Template مربوط به آن کلیک راست کرده و Copy را می زنیم و هربار مشخصات مربوط به هرکاربر را وارد می کنیم.
نکته : دقت کنید که User template ها همواره disable باشند.

Group :

به کمک گروه‌ها، مدیر شبکه می‌تواند یک مجوز دسترسی خاص (**Permission**) را به تعدادی **User** و یا حتی **Group** دیگر بطور همزمان اعمال کند؛ به جای آنکه مجوزها را برای تک‌تک افراد یا گروه ها، یکی یکی تعریف کند!

- پس می توان یک گروه رو عضوی از گروه دیگر کرد که به آن **Nested Group** گفته می شود.

گروه ها به دو شکل دسته بندی می شوند:

❖ بر اساس نوع کاربرد یا Group Type :

1. **Security** :

- به وسیله ی این گروه ها، می توان برای تعدادی از **Object** های شبکه، **permission** خاصی تعریف کنیم.
- این نوع گروه ها دارای یک **SID** هستند، یعنی شماره شناسایی.

نکته: اختصاص دادن Permission، همان تعریف Access Permission است، و با Access level فرق دارد.

2. **Distribution** :

- در حقیقت این گروه ها تنها برای ارسال ایمیل کاربرد دارند و قابلیت تعریف **Permission** را ندارند. هریک از این گروه ها، نوعی لیست برای ارسال ایمیل است، به همین جهت گاهی به گروه های **Distribution**، لیست **Distribution** گفته می شود. (**distribution list**)
- این گروه ها فاقد هرگونه **SID** هستند.
- در **Exchange Server** آنها را ایجاد کرده و تحت سیستم پست الکترونیکی مثل **Outlook** از آنها استفاده می کنیم.

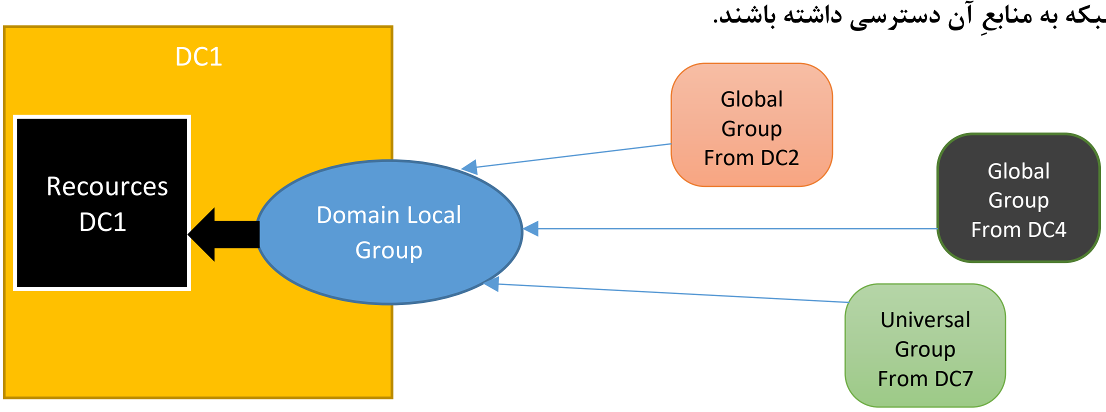
نکته: از گروه‌های security می‌توان به عنوان گروه‌های distribution به منظور ارسال ایمیل نیز استفاده نمود (که توصیه نمی شود)، اما برعکس آن ممکن نیست.

❖ بر اساس محدوده ی دسترسی یا Scope :

در حقیقت هرگروه، وظیفه دارد که یک سری منابع را برای یک سری User فراهم کند.

1. **Domain local** :

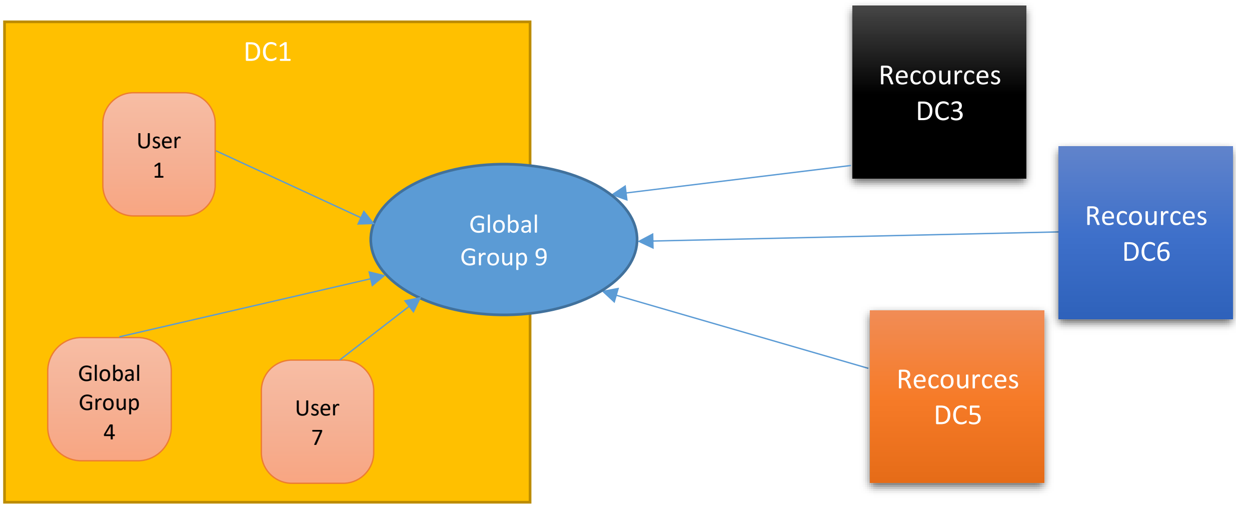
- می تواند به اعضایش **Access Permission** به منابعی که فقط در سطح **Domain** خودش هستند را بدهد.
- اما اعضای آن می توانند از **Domain** های دیگر موجود در کل **Forest** باشند.
- اگر یک **DL Group**، هیچ عضو **DL Group** ای نداشته باشد، می تواند به **Universal** تغییر داده شود.
- در حقیقت بهترین کار این است که منابع ضروری معمول در **main Domain** را عضو یک **DL Group** کنیم، تا همه ی اعضای کل شبکه به منابعِ آن دسترسی داشته باشند.



نکته: وقتی می گوییم یک گروه در سطح Domain کار می کند، یعنی فقط روی منابعی که در Domain خودش هستند کار می کند و یا اگر یک گروه در سطح Forest کار می کند، یعنی روی منابعی که در تمام یک Forest وجود دارند، کار می کند.

2. **Global :**

- **این گروه دسترسی به منابع موجود در تمام Forest را برای User های Domain خودش مدیریت کند.**
- **it can be assigned Permissions in any DC : از هر دومینی می تونه «مجوز» براش تخصیص داده بشه.**
- **چون منابع همه ی Domain ها می تونن در این گروه Share شده بشن.**
- **اما اعضای آن فقط می توانند از Domain خودش باشند و نمی‌تواند از Domain های دیگر عضو بپذیرد.**
- **گروه های Global فقط به یک شرط عضو یکدیگر می شوند که هردو در یک Domain باشند.**
- **اگر یک Global Group، هیچ عضو Global Group ای نداشته باشد، می تواند به Universal تغییر داده شود.**
- **بهترین کار این است که همه ی اعضای یک DC در گروهی Global عضو باشند تا به همه ی منابع دسترسی داشته باشند.**



اگر سعی کنید در AD Users and Computers برای یک گروه Global عضو بگیرید، می بینید که وقتی در تب Members وارد Add شده و Location را می زنید، فقط Object های همان Domain ای که در آن قرار دارد، قابل انتخاب هستند.

3. **Universal :**

- **فقط در سطح Forest خودش، کار می کند.**
- **از آن در Forest های بزرگ استفاده می شود.**
- **می‌تواند شامل تمام Object های موجود در کل Forest باشد.**
- **با استفاده از این گروه می توان Role تعریف کرد و منابعی که در بین چندین domain توزیع شده است را مدیریت کرد.**
- **اگر شبکه ی شما چندین شاخه دارد که به وسیله ی شبکه ی WAN متصل هستند، توصیه می شود که از Universal استفاده کنید.**
- **it can be assigned Permissions in any DC or Forest : از هر دومین یا جنگلی می تونه «مجوز» براش تخصیص داده بشه.**
- **اگر کوچکترین تغییری در یک گروه Universal صورت گیرد، فوراً در Global Catalog تمام شبکه replicate خواهد شد، پس استفاده ی بی مورد از این گروه‌ها باعث افزایش ترافیک شبکه می‌شود.**
- **نیازمند Global Catalog می باشد.مثلاً اگر User ای عضو اینگونه گروه باشد، برای log in کردن، باید دسترسی به Global Catalog Server داشته باشد.**
- **یک Universal Group، می تواند به یک Domain Local Group تبدیل شود و اگر هیچ عضو Universal ای نداشته باشد، به Global هم می تواند تغییر داده شود.**

نکته: بصورت قراردادی، برای نامگذاری گروه ها، در ابتدا اولین حرف نوع Scope آن گروه می آید، یعنی : DL یا G یا U .

: Default groups

Server Operators : گروهی است از نوع Domain Local که اعضای آن، دارای توانایی نصب و share کردن نرم افزار بر روی server و نیز مدیریت Disk ها و Back up های Server می باشند.

Account Operators : گروهی است از نوع Domain Local که اعضای این گروه توانایی ایجاد و مدیریت User ها و Group ها را در AD دارا هستند و همچنین می توانند User هایی که توسط اعضای دیگر این گروه ایجاد شده اند را delete کنند.

Print Operators : گروهی است از نوع Domain Local که اعضای این گروه توانایی نصب، share و مدیریت پرینترها هستند.

Administrators : گروهی است از نو ع Domain Local که اعضای آن، مدیر یا مدیرهای کامپیوتر Server هستند و برطبق عضویت در این گروه، قادر به همه ی امور کنترلی و مدیریتی Domain جاری هستند.

Backup Operators : این گروه از نوع domain local می باشد و اعضای آن توانایی بکاپ گیری و Restore کردن Back up ها بر روی server را دارند، بدون اینکه لزوما توانایی هایadmin را داشته باشند.

Network configuration Operators : یک گروه Domain Local است که اعضای آن توانایی تعیین سطوح مدیریتی شبکه را دارند. بصورت پیشفرض عضوی ندارد و خودش نیز عضو گروهی نیست.

Remote Desktop Users : اعضای این گروه می توانند به صورت Remote Desktop متصل شوند.
Remote Management Users : اعضای این گروه می توانند به صورت Remote (مثل برقراری Session) متصل شوند.
Domain Computers : یک گروه Global می باشدکه شامل همه کامپیوترهای عضو دامین، شامل Client ها و Server ها با هر نسخه ای از هر سیستم عاملی می باشد.هر کامپیوتری که join دامین شود، بصورت خودکار عضو این گروه می شود، به جز کامپیوترهای DC که به گروه Domain Controllers منتقل می شوند.

Domain Users : گروهی است global شامل تمام یوزرهای دامین.خود این گروه عضو گروه users می باشد.

Domain Admins : این گروه global است و اعضای آن دارای قابلیت administrator هستند که می توانند هر کاری انجام دهند.

Enterprise Admins : گروهی است از نوع Universal که اعضای آن دارای اختیارات کامل مدیریتی در سراسر forest و نه فقط در Domain می باشند.

: Add Users or Groups to a Group

- برای مشاهده ی اعضای یک Group (مثلاً گروه G1) :

```
Get-ADGroupMember -Identity G1 | ft name,distinguishedName
```

روش اول: روی User یا Group مورد نظر، کلیک راست کرده و Add to a Group را می زنیم.
روش دوم: وارد Properties گروه یا یوزر مورد نظر می شویم و در تب Member of، گروه مقصد را انتخاب می کنیم.
روش سوم: وارد Properties گروه مقصد می شویم و در تب Members، برای آن عضو انتخاب می کنیم.

اما برای حذف یکی از اعضای یک گروه، گاهی این Error را می دهد که این گروه، به عنوان Primary Group برای این کاربر است!
در این مواقع، باید وارد Properties کاربر موردنظر شده و در تب Member of، یک گروه دیگر را به جز آن گروه، انتخاب کرده و در پایین، دکمه ی Set Primary Group را بزنیم.
سپس می توان آن کاربر را از Group موردنظر، حذف کرد.

توسط PowerShell :

- برای عضو کردن یک یا چند User دریک گروه به نام G1 :

```
Add-ADGroupMember -Identity G1 -Members UserName1,UserName2
```

نکته: اگر تعداد Group ها و تعداد User ها خیلی زیاد باشد، می توان به کمک تهیه ی مشخصات آنها در یک فایل CSV هم این عضویت را انجام داد.

AGDLP Rule :

این تکنیک برای محیطهای single Forest و single Domain کاربرد دارد.
Account ها را عضو گروه Global می کنیم.
گروه های Global را عضو گروه Domian Local کرده و Permission نهایی را همیشه به گروه Domain Local می دهیم.
در حقیقت هرکجا خواستیم Access Permission بدهیم، به Domain Local می دهیم.
طبق گفته ی Microsoft این قانون را برای شبکه هایی با بیش از 500 کاربر، استفاده می کنیم.

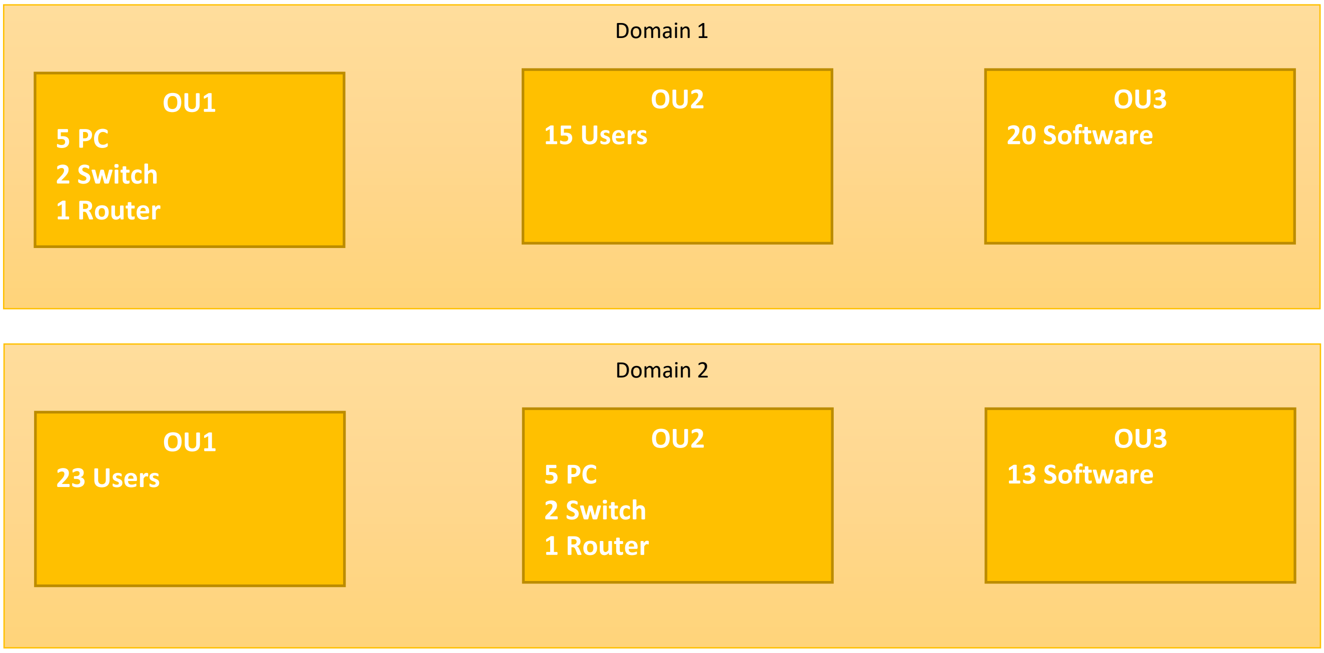
AGUP Rule :

همیشه Account ها را عضو گروه Global می کنیم.
و همیشه گروه های Global را عضو گروه Universal کرده و Permission نهایی را به گروه Universal می دهیم.
در حقیقت این قانون برای زمانی ست که Resource های شبکه در محدوده های مختلفی از داخل و خارج از Domain جاری هستند.
این قانون معمولاً در Forest ای که یک Domain دارد، بی کاربرد است.

AGUDLP Rule :

: (Organizational Unit) OU

یک گروه یا چهارچوب است که می توان با توجه به سیاست های مورد نیاز، درون آن تعدادی **user** و **computer** قرار داد.
در حقیقت به محض نصب **AD DS** ، اولین **OU** بصورت خودکار ایجاد می شود.
به طور پیشفرض یک **OU** وجود دارد به نام **Domain Controllers** که شامل **Domain Controller** های شبکه خواهد بود.



فرض کنید درشبکه ای با 300 حساب کاربری، مدیرشرکت تصمیم می گیرد که بیانیه ای را به کاربران بخش بازاریابی اعلام نماید و می خواهد این بیانیه بصورت متن در هنگام **log on** شدن کاربران آن بخش، به آنها نمایش داده شود.
تنها کاری که باید انجام شود، اینست که یک **OU** ایجاد شده و همه ی اکانت های متعلق به کارکنان بازاریابی را درون آن فرستاد.
حال برای **OU** فوق یک **policy** تعریف می کنید که متن موردنظر، هنگام اولین **log on**، برای هر کاربر به نمایش درآید.

OU ها براساس سه معیار بوجود می آیند:

- کاربرد (متداول ترین)
- **Secure Levels**
- جغرافیا (کمتر متداول است)

برای ساخت **OU** در کنسول **AD users and computers** از پنل سمت چپ، **Root Domain** را انتخاب کرده، و سپس در پنل سمت راست آن، در یک فضای خالی، راست کلیک کرده، گزینه **new** و سپس **organization Unit** را انتخاب کنید.

نکته: درون محیط خود **OU** هم می توان دوباره **OU** ساخت و سلسله مراتبی از **OU** ها را ایجاد کرد.

برای جابجایی **User** ها، یا با **Drag** کردن می توان و یا کلیک راست و **move** !

نکته: اعضای یک **OU** می توانند از گروه ها، **Domain** ها و سایت های مختلف باشند، اما **Policy** هایی که به یک **OU** اعمال می شود، روی تک تک اعضای آن اعمال می شوند، بدون اهمیت به اینکه از کدام **domain** یا **site** هستند.

ایجاد یک OU :

نکته: برای ایجاد OU توسط **PowerShell**، مسیر ایجاد **OU** باید به شکل **Distinguish** درج شود.

اگر **OU** در زیرمجموعه ی خودِ **Domain** باشد و نه هیچ پوشه یا **OU** دیگر، آدرس آن، همان آدرس **Root Domain** می باشد.

برای ایجاد یک OU در دامین payamavar.local:

```
New-ADOrganizationalUnit -Name نام  -Path "dc=payamavar,dc=local"
```

ایجاد یک User در یک OU :

```
New-aduser -name "A B"-Givenname A -Surname B -SamAccountname AB -UserPrincipalName AB@payamavar.local
-Path “ou=persons,dc=payamavar,dc=local”
```

برای اینکه توسط **PowerShell** درون فضای **Active Directory** بتوانیم جستجو کرده و میان **OU** ها جابجا شده و محتویات آنها را مشاهده کنیم:

- ابتدا **Module** آن را وارد می کنیم:

```
Install-Module ActiveDirectory
```

- وارد **AD** می شویم:

```
cd ad:
```

- وارد **Domain** موجود در **Active Directory** می شویم. ابتدا خط زیر را درج کرده و سپس توسط دکمه ی **Tab**، آن را جابجا می کنیم و روی مسیر صحیح **Domain** شبکه نگه داشتیم و وارد می کنیم.

```
cd dc =
```

- وارد به شکل دستور قبل، وارد مسیر **OU** موردنظر می شویم.

```
cd ou =
```

- توسط دستور **dir** می توانیم محتویات هر مسیر را ببینیم.

: Delegating OU

فرض کنید که در یک شبکه ی Domain، چند DC وجود دارد.
در AD این شبکه، یک OU خاص داریم که شامل تعدادی عضو هم می باشد، و قصد داریم کنترل این OU را فقط به دست یک یا تعدادی عضو خاص از شبکه اعطا کنیم و هرکسی که وارد یکی از DC ها شد، قادر به تغییر در OU مورد نظر نباشد.

1. یک Group مثلاً به نام G1 ایجاد می کنیم.(مثلاً از نوع Domain Local و Security)
2. آن عضو یا اعضایی که تنها آنها باید توانایی ایجاد تغییر در OU مورد نظر را داشته باشند را، عضو G1 می کنیم.
3. روی OU کلیک راست کرده و Delegate Control را می زنیم.
4. سپس Add را زده و گروه G1 را وارد می کنیم و Next.
5. سپس دسترسی ها یا وظایفی که می خواهید را انتخاب می کنید و Next .

نکته: بهتر است که خود گروه G1 هم درون OU قرار داشته باشد.

:Group versus OU

- می توان روی OU ها از طریق Group policy، قوانین متنوعی تعریف کرد، ولی روی Group ها نمی توان.
- هرگاه بخواهیم یک Policy را به تعدادی Object اعمال کنیم، آبجکت های فوق را درون یک OU قرار می دهیم و سپس Policy را روی OU اعمال می کنیم؛ و هرگاه بخواهیم permission به دو یا چند عضو اختصاص دهیم، Objectd ها را در گروه مورد نظر عضو کرده و permission را به گروه نسبت می دهیم.
- یک Group را می توان درون OU قرار داد، ولی نمی توان یک OU را به عضویتِ یک Group در آورد.

: Container

علاوه بر OU ها و Group ها، می توان Object های اکتیودایرکتوری را توسط Container ها نیز طبقه بندی و دسته بندی کرد.
تعدادی Container بصورت پیش ساخته (Built-in) در AD تعریف شده اند که به محض نصب AD DS در دسترس هستند.
Container های پیش ساخته عبارتند از:

- Computers : شامل تمام کامپیوترهای Domain است.
- Builtin : شامل تمامی آبجکتهای پیش ساخته است.
- Managed Service Accounts : دربرگیرنده ی حساب های سرویسی مدیریت شده است.

نکته: می توان Object های درون یک Container را به داخل یک OU انتقال داد.
نکته: می توان Group Policy Object ها را به OU ها اعمال کرد ولی به Container ها نمی توان اعمال کرد.

:Bitlocker Tab

برای اینکه تنظیمات Bitlocker یک کامپیوتر عضو Domain، در پنجره ی Properties آبجکت آن، به شکل یک تب جداگانه، ظاهر شوند، دستور زیر را در PowerShell سیستم Server وارد می کنیم:

```
$objComputer = Get-ADComputer PCNAME
$Bitlocker_Object = Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} -
SearchBase $objComputer.DistinguishedName -Properties 'msFVE-RecoveryPassword' $Bitlocker_Object
```

Users and Groups PowerShell-Support :

-مثال

فرض کنید:

یک سری **User** در **OU1** داریم.

یک سری **Group** در **OU4** داریم.

می خواهیم بررسی کنیم که آیا هیچ یک از **User** های موجود در **OU1** عضو هیچ یک از گروه های موجود در **OU4** هستند یا خیر.

پس نتیجه را به این شکل تعریف می کنیم که:

- **User** های عضو در گروه ها، در یک فایل لیست شوند.
- و **User** هایی که کامل چک می شوند و عضو هیچ گروهی نیستند، در یک فایل جداگانه لیست شوند.

```
$USERS= Get-ADUser -Filter * -SearchBase 'OU=OU1,OU=Users,DC=payamavar,DC=local' -Properties
"SamAccountName","distinguishedname" | select SamAccountName -ExpandProperty SamAccountName | sort

foreach($U1 in $USERS){
        $username0 = $U1
        $group0 = Get-ADGroup -Filter * -SearchBase 'OU=OU4,OU=Users,DC=payamavar,DC=local'
         -Properties name | select Name -ExpandProperty name | sort
         foreach($GRP in $group0){
        $USR = Get-ADGroupMember -Identity $GRP | Where-Object {$_.samaccountname -eq $username0}
        if($USR){
                "member found , the Account  $username0 is in $GRP." | Add-Content -Path
                 "Z:\FoundPersonal.txt"
                    }
            else{
                 "member not found , the Account  $username0 is not in $GRP." | Add-Content -Path
                 "Z:\notFoundPersonal.txt"
                     }
                                  }
                       }
```

-مثال

می خواهیم تمام **User** های موجود در یک مسیر از **AD** را، که نه **deactived** و نه **expired** هستند و طی **90** روز گذشته و یا حتی بیشتر، در شبکه **login** نکرده اند، بیابیم.

```
$ou="OU=OU1,OU=Users,DC=payamavar,DC=local"
Get-ADUser -Filter {Enabled -eq $true} -SearchBase $ou -Properties
Name,SamAccountName,LastLogonDate,LastLogon | select SamAccountName,LastLogonDate,
distinguishedname | Where {($_.LastLogonDate -lt (Get-Date).AddDays(-90)) -and
($_.LastLogonDate -ne $NULL)} | Sort | Select SamAccountName, LastLogonDate, distinguishedname
```

-مثال

می خواهیم تمام User هایی که در یک OU و همچنین در تمام OU های زیرمجموعه ی آن، باطل یا **expired** شده اند را بیابیم.

```
Search-ADAccount -AccountExpired -UsersOnly -SearchBase "OU=OU1,OU=Users,DC=payamavar,DC=local"
-SearchScope Subtree | FT Name,ObjectClass,distinguishedname
```

-مثال

می خواهیم تمام User های موجود در یک مسیر از AD را، که **deactivated** هستند، بیابیم.

```
Get-ADUser -Filter {Enabled -eq $false} -SearchBase "OU=OU1,OU=Users,DC=payamavar,DC=local" |
FT samAccountName, distinguishedname
```

-مثال

می خواهیم تمام User های موجود در یک مسیر از AD را، که یک **attribute** آنها خالی است (مقداری ندارد) را بیابیم.

مثلاً : mailNickname

```
Get-ADUser -Filter * -SearchBase "OU=OU1,OU=Users,DC=payamavar,DC=local" -Properties
mailNickname | where mailNickname -like "" | select SamAccountName, mailNickname
```

-مثال

می خواهیم تمام User های موجود در یک مسیر از AD را، که **User name** آنها شامل چند حرف یا یک کلمه ی خاص است را بیابیم.

مثلاً: کلمه ی admi

```
Get-ADUser -Filter * -SearchBase "OU=OU1,OU=Users,DC=payamavar,DC=local" `
-Properties name, SamAccountName, city | where SamAccountName -Like "*admi*" | select
SamAccountName, name, city
```

-مثال

می خواهیم تمام User های موجود در یک مسیر از AD را، که در **description** آنها، یک کلمه ی خاص درج شده است را بیابیم.

مثلاً: کلمه ی LITP

```
$list0= Get-ADUser -Filter * -SearchBase "OU=OU1,OU=Users,DC=payamavar,DC=local" `
-Properties description | where description -Like "*litp*" | select SamAccountName `
-ExpandProperty SamAccountName | sort
    $i = 1
    foreach($a0 in $i){
    Write-Host $i : $a0
    $i++
    }
```

-مثال

می خواهیم اعضای یک **Group** را دریافت کنیم:

```
Get-ADGroupMember -Identity "DAR1_Office_Director" | select -ExpandProperty samaccountname
```

-مثال

می خواهیم ببینیم آیا یک **User** عضو یک **Group** هست یا خیر:

```
$username = "payam.avar"
$group = "NIX1_Office_Director"
$user = Get-ADGroupMember -Identity $group | Where-Object {$_.samaccountname -eq $username}
if($user){
Write-Host $username IS A Member of $group .
}else {
Write-Host $username is NOT a member of $group .}
```

-مثال

می خواهیم گروه هایی که یک User عضو آنهاست را لیست کنیم:

```
$GRP1 = Get-ADPrincipalGroupMembership "payam.avar" | Select name -ExpandProperty name | sort
; $i=1 ; foreach($cal2 in $GRP1) { Write-Host "$i : $cal2" ; $i++ }
```

-مثال

با توجه به اینکه گاهی چندین Group با اسامی مشابه وجود دارند. می خواهیم در یک مسیر از AD، تمام member های تمام Group هایی که در نام آنها کلمه ی Office وجود دارد را لیست کنیم.

```
$group0 = Get-ADGroup -Filter * -SearchBase "OU=OU1,OU=Users,DC=payamavar,DC=local"
-Properties name  | where name -Like "*Office_Director*" | select Name -ExpandProperty name | sort
  foreach($GG in $group0)
  {
  Write-Host "--------------------------------"
  Write-Host "-----------" $GG ':'
  Get-ADGroupMember -Identity $GG | select samaccountname -ExpandProperty samaccountname | sort
  }
```

Add a PC to Domain :

دو روش برای عضو کردن یک سیستم در یک شبکه وجود دارد:

- **Staged** : مدیر کل **Domain**، شخصاً در پشت سیستم **Client** یا **member Server** دست بکار شده و با مشخصات کاربری خودش، سیستم را به **Domain** اضافه می کند.
- **Pre-Staged** یا **Non-Staged** : یک شخص به عنوان **Local Admin**، در محل حضور دارد و با مشخصات کاربری مخصوص که مدیر کل **Domain** برای او در سرور اصلی تعریف کرده است، سیستم را به **Domain** اضافه خواهد کرد.

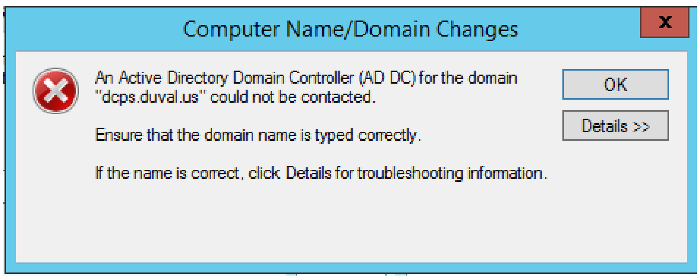
Staged :

روش GUI :

1. یک اتصال کابلی بین سوئیچ و **PC** برقرار می کنیم.
2. باید در بخش **Change Adapter Setting**، دریافت **IP** را بصورت **Automatic** و از **DHCP** تنظیم کنیم و برای آدرس **DNS** اول، آدرس **IP** کامپیوتر **DC** را وارد کنیم.
3. وارد **cmd** شده و به سیستم **Domain Controller** یکبار **Ping** می کنیم.اگر اعلام قطع ارتباط کرد، باید یکبار حافظه ی **DNS** را پاک کنیم.
4. پس تایپ می کنیم: **ipconfig /flushdns**
5. و دوباره به **Domain Name** پینگ می کنیم تا از برقراری ارتباط صحیح با **DC** مطمئن شویم.

6. به **Control Panel < System < Change Setting < Change** رفته و جدا از اینکه **Computer Name** چه است، تیک **Domain** را فعال کرده و **Domain Name** را درج کرده و **Ok** کرده و اطلاعات **user** و **pass** که در **Active Directory** برای آن کاربر ساختیم را وارد می کنیم و سیستم را **reset** می کنیم.

گاهی با **Error** زیر مواجه می شویم که نشان از مشکل در ارتباط با **Domain DNS** دارد.



- در کامپیوتر **Server** پنجره ی **cmd** را باز کرده و سرویس **netlogon** را یکبار **reset** می کنیم.
- به این صورت که اول درج می کنیم: **Net stop netlogon**
- سپس درج می کنیم: **net start netlogon**
- و دوباره امتحان می کنیم.
- اگر باز هم نشد، با دستور **ipconfig /flushdns** در **CMD**، باید **DNScache** را **reset** کنیم.
- و احتمالا نیاز به **reboot** کردن سیستم **Client** هم خواهد بود.

نکته: همیشه، بعد از تغییر به حالت Domain، اولین ورود تحت Domain را با اکانت Administrator مربوط به کامپیوتر Server انجام می دهیم.
پس به این شکل یوزر را وارد می کنیم :

Domain Name \ Administrator یا و Root Domain address

پس از یکبار ورود، و اطمینان از عضویت در Domain، دوباره reset می کنیم و اینبار با User خاص تعریف شده از قبل، وارد می شویم.
به شکل مقابل user را وارد کرده و سپس پسورد و اینتر: Domain Name \ Account Name

- **البته در دفعات بعد، نام Domain، بطور ثبت شده خواهد بود، و فقط کافی ست نام user تعریف شده را بنویسیم، یعنی فقط درج Password و اینتر.**
- **اگر در آینده بخواهیم توسط یک حساب Local Administrator و یا یک Local Account وارد شویم، باید نام Account را به یکی از حالات زیر وارد کنیم:**

Computer Name \ Account Name

.\ Account Name

بعد از join شدن یک سیستم به Domain، در AD DS، آبجکت آن، با نام آن کامپیوتر، اضافه می شود.
همانطور که می دانیم برای تغییر نام هریک از سیستمها، باید درون آن سیستم وارد Control Panel و System شد.
اما برای اینکه درون DC نام آن را به سادگی عوض کنیم، کافی ست در cmd دستور زیر را درج کنیم:

netdom renamecomputer pc1 /newname:Comp1 /force

روش PowerShell :

چه یک سیستم و چه چند سیستم، می توانیم همگی را با همین یک Syntax عضو Domain کنیم.
نکته: باید Firewall روی آنها خاموش باشد.
نکته: از یک Admin User در Domain استفاده می کنیم.
نکته: باید رمز عبور حساب local Administrator در همه ی سیستم های موردنظر، یکسان باشد که دردسرساز نشود!

```
Add-Computer -ComputerName Comp1 -DomainName Payamavar.local -LocalCredential Administrator
-Credential PAYAMAVAR0\Administrator -Restart -Force
```

بعد از وارد کردن این دستور، ابتدا پسورد Local Administrator را درخواست می کند.
می توانیم نام کامپیوترهای بیشتری را نیز وارد کنیم:

```
-ComputerName Comp1,Comp2,Comp3
```

برای حذف یک کامپیوتر از Domain:

```
Remove-Computer -ComputerName Comp1 -LocalCredential Administrator
-UnjoinDomainCredential Payamavar.local -Credential PAYAMAVAR0\Administrator
-WorkgroupName "WG" -Force
```

- **به دلخواه یک نام Workgroup برای آن درج می کنیم.**

برای مشاهده ی همه ی Computer های عضو شبکه و یا فقط Computer های فعال شبکه:

```
Get-ADComputer -Filter *
Get-ADComputer -Filter 'enabled -eq "true"'
```

- **برای تغییرنام یک Computer عضو شبکه، طوری که هم در خود آن PC و هم در AD نامش عوض شود:**

```
Rename-Computer -ComputerName "192.168.139.145" -NewName "NewName" -Force -Restart
```

: Pre-Staged

- یک اتصال کابلی بین سوئیچ و PC برقرار می کنیم، و یا به یک طریقی آنها را به هم وصل و آدرس دهی می کنیم که بتوانند به یکدیگر Ping شوند.
- با هماهنگی با کاربری که با عنوان Local Admin پشت سیستم Client است، یک نام برای این Computer انتخاب می کنیم.
- در سیستم Server ، یک User معمولی برای Local Admin ایجاد می کنیم.
- بر روی آبجکت Main DC در AD Users and Computers کلیک راست کرده و delegate Control را زده و این User مربوط به Local Admin را Add کرده و task مربوط به Join a Computer to the Domain را انتخاب و فعال کرده و Finish!
- سپس در همان AD Users and Computers در یک Container یا OU دلخواه، کلیک راست کرده و new Computer را زده و بالاخره نام موردنظر برای آن کامپیوتر Client را وارد کرده و سپس برای گزینه ی User or Group روی دکمه ی Change کلیک کرده و User ایجاد شده برای Local Admin را انتخاب می کنیم و Next و Finish.
- Local Admin:
  - باید DNS Server Address را مطابق با DNS Server شبکه وارد کند.
  - در درون آن سیستم، به Control Panel رفته و در System مسیر زیر را طی کند:

Change Setting > Network ID > This Computer is part of a business Network,... > My Company uses a network with a Domain > نام و پسورد حساب کاربری که مدیر در سرور برایش ایجاد کرده است.> Domain Name

نکته: می توانیم برای User name، نام User را همراه با FQDN مربوط به DC وارد کنیم (User1@payamavar.local) که دیگر نیازی به وارد کردن مقداری برای فیلد Domain name نخواهد بود؛ و یا فقط نام User را وارد می کنیم.

- در ادامه، نوع این سیستم را Standard قرار داده و Finish و یکبار سیستم باید Restart شود.

نکته:

فرض کنید، پس از عضو شدن یک PC در Domain وساخته شدنِ یک گزینه به نامِ آن PC در بخش AD Users and Computers، مدیر شبکه، این گزینه ی PC را با یک کلیک راست و Delete، حذف کند.

در نتیجه اگر فقط یکبار در کامپیوتر مورد نظر Sign out کنیم و قصد sign in داشته باشیم، Error می دهد.

از طرفی اگر قصد کنیم با User محلی خود PC وارد شویم هم Error می دهد!

پس باید نام local User را به شکل زیر درج کنیم و سپس پسورد و تمام!

PC Name\Local Account Name

برای ایجاد یک Object Computer در PowerShell :

```
New-ADComputer -Name bbb -DNSHostName bbb.payamavar.local -Enabled $true
-Path "OU=PCs,DC=payamavar,DC=local"
```

نکته: مقدار Name باید حتماً برابر با Computer Name سیستم مقصد باشد.

:Redirection

فرض کنید یک OU ایجاد کرده ایم به نام Clnt، حال برای اینکه به صورت Default، کاربرهایی که به شبکه متصل می شوند، Object آنها، در این OU ایجاد شوند، وارد cmd شده و توسط Distinguished Name مربوط به OU موردنظر، دستور زیر را درج می کنیم:

Redircmp "OU=Clnt,DC=Payamavar,DC=local"

اگر پاسخ زیر بیاید، پس از این به بعد هر Client ای که عضو Domain شود، وارد این OU می شود.

Redirection was Successful.

Domain Remote Desktop :

از این به بعد، هر کامپیوتر، علاوه بر اینکه یک IP منحصربفرد دارد، یک Name منحصربفرد نیز دارد که بصورت زیر است:
Root Domain Address و یا Computer Name.Domain Name
مثلاً کامپیوتر PC1 در شبکه ای با آدرس Root مقابل: Payamavar.local
PC1.payamavar.local
به همین جهت، در برنامه ی Remote Desktop برای وصل شدن به یک کامپیوتر، می توان به جای IP از Name آن نیز استفاده کرد.

- برای اینکه یک کامپیوتر بتواند از قابلیت Remote Desktop و قابلیت های مدیریتی دیگر در یک سیستم استفاده کند، باید آن را در گروه **Domain Admins** نیز عضو کرد.

نکته: برای اینکه بتوانیم به سیستم های دیگر ارتباط Remote Desktop بزنیم، باید در آنها Power Plan را برای Turn off و Sleeping بر روی Never قرار داد.

(ODJ) Offline Join to the Domain :

ابتدا باید یک فایل در Server ایجاد کنیم و سپس در Client آن را اجرا کنیم، که در هر دو طرف، توسط cmd انجام می شود.
نکته: تمام سیستم هایی که در شبکه، به عنوان Server عضو Domain هستند، باید روشن باشند، در غیراینصورت، Djoin کار نمی کند.

در Server، کنسول CMD را بصورت Administrator باز کرده و درج می کنیم:
Djoin /provision /domain آدرس روت دومین /machine نام کامپیوتر کلاینت مقصد /savefile آدرس و نامی برای ذخیره ی فایل
Djoin /provision /domain Payamavar.local /machine PC3 /savefile c:\new folder\ABC

نکته: اگر سیستم موردنظر، قبلاً عضو Domain بوده و جدا شده و حال می خواهیم از طریق ODJ دوباره آنرا متصل کنیم، باید همه ی Metadata های قبلیِ آن حذف شده باشند و سپس دستور بالا را با یک سوییچ اضافه تر در انتها وارد می کنیم: /reuse

سپس به هرشکل ممکن، این فایل ایجاد شده را در کامپیوتر Client که هنوز هم عضو Domain نشده است، کپی می کنیم.
حال در Client، cmd را حتماااااا **با دسترسی Admin** باز می کنیم و درج می کنیم و یکبار Restart:
djoin /requestodj /loadfile آدرس و نام فایل /windowspath %systemroot% /localos
djoin /requestodj /loadfile c:\pop /windowspath %systemroot% /localos

نکته: در صورت عدم موفقیت در اجرای این دستور، نیاز است که UAC را باز کرده و میزان آن را به حداقل برسانید!

Sharing and Access :

- برای Share کردن یک فایل یا پوشه، وارد Properties آن شده و در تب Sharing، وارد Advanced Sharing می شویم.
- برای اینکه مشاهده ی یک پوشه ی Share شده برای کسی ممکن نباشد، در انتهاب Share Name ای که برای آن درج می کنیم، یک $ قرار می دهیم.

- وقتی صحبت از Share Permission ها می کنیم، منظور تعیین سطح دسترسی در سطح شبکه است، در حقیقت، از طریق همان دکمه ی Advanced Sharing، سطح Sharing Permission را مشخص می کنیم.

- وقتی صحبت از NTFS Permission ها (Security Permission) می کنیم، منظور، تعیین سطح دسترسی هم در سطح شبکه و هم در سطح خود کامپیوتر هست.

مثلاً شما برای یک Folder می توانید از طریق NTFS Permission ها حتی تعیین کنید چه کسانی بر روی همان کامپیوتر (البته در سطح شبکه) دسترسی داشته باشند.
در حالی که از طریق Share Permisson ها تنها می توان تعیین کرد چه کسانی در سطح شبکه، اجازه ی دسترسی به آن را داشته باشند.

- برای NTFS Permission های یک File، روی آن کلیک راست کرده و Properties را زده و وارد تب Security می شویم.
روی دکمه ی Advanced زده و در پنجره ی باز شده می بینیم که بطور Default، این فایل را برای دو گروه System و Administrators و همچنین User ها، به اشتراک گذاشته است!
در حقیقت این سه sharing باقی خواهند ماند، مگر اینکه در پایین همین پنجره، گزینه ی Disable Inheritance را بزنیم.
روی Add کلیک می کنیم و سپس گزینه ی Select a Principal را می زنیم.
حال گروه یا User مورد نظر را پیدا و انتخاب می کنیم.
نکته: در همین کنسول Advanced Security Setting می توان Share Permissions را در درون تب Share هم تعیین کرد.

- مجوزهای File ها در اولویت تر از مجوز Folder هاست.
مثلاً زمانی که یک User به یک File که درون یک Folder است، دسترسی داشته باشد اما به خود Folder دسترسی نداشته باشد، می تواند به File دسترسی پیدا کند. اما از طریق آدرس UNC آن:
در شبکه : \\Computer_name\share\File
به صورت محلی : C:\folder\file

- Deny در اولویت تر از Allow است.
- اگر NTFS Permission و Share Permission را به صورت همزمان برای یک فایل تنظیم کنیم، هرکدام که محدودکننده تر باشد، در اولویت تر خواهد بود.

معرفی Permission ها:

- Change : کاربر دارای این مجوز، می تواند نام و محتویات فایل را تغییر داده و حتی حذف کند.
- Read : کاربر دارای این مجوز، می تواند فقط فایل را ببیند و اگر Application باشد، فقط می تواند آنرا اجرا کند.
- Full Control : کاربر دارای این مجوز، علاوه بر ویژگی های دو مجوز قبل، تمام قابلیت هایی که Owner یا صاحب آن فایل دارد را نیز خواهد داشت. مثل تعیین Permission ها.
- برای اینکه بتوانیم یک فایل را ببینیم، حتما به مجوز Read نیاز خواهد بود، حتی اگر مجوز write را داشته باشیم.
- اگر برای یک فایل، مجوز Full NTFS Permission را داشته باشیم، اما Full Share permission را نداشته باشیم، همچنان نمی توانیم ownership آن فایل را دریافت کنیم.

برای دسترسی به محتویات shared شده ی یک کامپیوتر در شبکه، یا درون پنجره ی RUN و یا در یک Explorer، درج می کنیم:

\\\\ Name و یا IP

برای دسترسی به پارتیشنی از یک سیستم عضو شبکه، که آن پارتیشن Share نشده است، علاوه بر IP آن سیستم، نام پارتیشن موردنظررا همراه با علامت $ درج کرده و اینتر می زنیم. مثلاً برای درایو E یک سیستم با IP فرضی زیر:

\\\\192.168.22.73\E$

برای وارد به پارتیشنی از یک سیستم عضو شبکه که البته آن پارتیشن را Share کرده است، مثلاً برای پارتیشن C :

\\\\192.168.22.73\C

Shared Folders :

یکی از ابزارهای مدیریت فایل های Share شده، کنسول Shared Folder می باشد.
می توان آن را توسط نامش در فرمان Run به نام fsmgmt.msc فراخوانی کرد، و یا در MMC و توسط Add Snap in ، گزینه ی Shared Folder را اضافه می کنیم.
می بینیم که سه بخش دارد.

Shares :

شامل تمامی Data هایی ست که روی سیستم Share کرده ایم.
در حقیقت تمام پوشه هایی که در کل سیستم share شده اند، در این قسمت قرار دارند.
در حقیقت نوعی اشتراک گذاری وجود دارد به نام Hidden Share که شامل پوشه هایی می شود که به صورت Hidden، و یا با نام های خاص به اشتراک گذاشته شده اند، می شود.
Hidden Share ها در قسمت Shared Directory دیده نمی شوند، اما در صورت فراخوانی آنها با درج نام شان، قابل باز شدن و دیده شدن هستند.
نکته: بطور پیشفرض، فقط کاربرهای Admin قادر به فراخوانی و دسترسی به Hidden Share ها هستند.
نکته: در حقیقت مزیت بزرگ پوشه ی Shares این است که Hidden Share ها را نیز نشان می دهد.

- ستون Share Name، نامی را نشان می دهد که هر فایل، با آن نام Share شده و قابل دسترسی در شبکه است.
- ستون Folder Path، آدرس دقیق فایل یا پوشه ای که Share شده است را نشان می دهد.
- ستون Client Connection نشان می دهد که همزمان چه تعداد User به آن فایل share شده دسترسی دارند.

نکته: در انتهای Share Name مربوط به فایل های Hidden Share، یک $ قرار می گیرد، که می توانیم خودمان هم این کار را انجام دهیم.

- همانطور که می بینیم همه ی Drive های سیستم، بطور پیشفرض Hidden Share هستند که در Description آن درج شده است!
- در حقیقت، نمی توان به Default Share ها، هیچ نوع Share Permission ای اعمال کرد.
- برای حذف Sharing هریک از فایل ها، می توان کلیک راست کرده و Stop Sharing را زد.
- برای ایجاد یک Shared File کافی ست در صفحه ی Shares کلیک راست کرده و New Share را بزنیم.

نکته: البته برای مشاهده ی فایل ها و پوشه های Share شده ی سیستم، می توان از دستور Net Share نیز در cmd استفاده کرد.

Sessions :

در این قسمت، تمام Session ها یا Connection هایی که به این سیستم زده شده است را مشاهده می کنیم.
این ارتباط یا Session می تواند شامل استفاده و دسترسی یک Client از یکی از File هایی که Share کرده ایم هم باشد!

Open Files :

در این قسمت، می توانیم ببینیم که Client های متصل شده، کدام فایل ها را اجرا کرده اند.

:File and Storage Services

برای انجام و یا کنترل Sharing، می توان وارد Server Manager شده و از سمت راست گزینه ی **File and Storage Services** را زد. در گزینه ی **Share**، محتوای **Share** شده را می بینیم.

اما برای اینکه بتوان محتوای DC های دیگر را در این محیط مشاهده و کنترل کرد، باید Role های SMB و NFS درون آنها نصب باشند:

```
Install-WindowsFeature fs-fileserver
Install-WindowsFeature fs-nfs-service
```

- با کلیک راست بر روی هریک از فایل های Share شده، می توان آنها را دید و یا Sharing آنها را قطع کرد و یا وارد **Properties** آنها شد:
  - در تب **Permissions** می توانیم **NTFS Permissions** را تعیین کنیم یا تغییر دهیم.
  - در تب **Setting** :

    توسط فعالسازی گزینه ی **Enable Access-based enumeration**، اظهار می کنیم که اگر کاربری به فایل **Share** شده ای دسترسی ندارد، نیازی هم نیست که آن را ببیند.

    توسط فعالسازی گزینه ی **Allow Caching**، به سرعت عمل سیستم کمک می شود.

نکته: برای به اشتراکگذاری فایل های حافظه های مجازی یا **VHD** و یا **Partition** های خود سیستم، در این تب فقط می توان آنها را **Encrypt** کرد و بقیه ی گزینه ها خاموش خواهند بود.

- برای ایجاد یک **Share** جدید، در بالا، وارد **Tasks** شده و **New Share** را می زنیم.

نکته: همانطور که می بینیم، به طور کلی، این **Share Profile** ها به دو دسته ی **SMB** و **NFS** تقسیم می شوند.

- SMB (Server Message Block): برای سیستم های مایکروسافتی و تا حدی **Apple** بکار می رود.
- NFS (Network File Service): برای سیستم های لینوکس و یونیکس بکار می رود.

- **SMB Share - Quick** : برای اشتراک گذاری کلی و فوری بکار می رود.
- **SMB Share – Advanced** : اشتراک گذاری را همراه با تعریف **Policy** های خاص برای پوشه ها و **User** های خاص انجام می دهد و توسط قابلیت **Quotas** می توان تعیین کرد که هرکاربر تا چه میزان می تواند درون یک پوشه، فایل ایجاد کند.

در **PowerShell** هم می توان این اشتراک گذاری ها را انجام داد.

: SMB Share

برای دریافت Cmdlet های SMB و NFS می توانیم درج کنیم:

```
Get-Command -Module SmbShare
Get-Command -Module nfs
```

- مثلاً توسط دستور زیر Share Permission ها را برای یک پوشه تنظیم می کنیم:

نکته: برای استفاده از هر User یا گروهی که تحت شبکه باشد، باید نام Domain ای آن را وارد کنیم، در غیراینصورت، فقط برای سیستم local عمل خواهد کرد.

```
New-SmbShare -Path 'F:\My Comments' -Name cmts -FolderEnumerationMode AccessBased
-FullAccess 'payamavar0\Domain Admins'
-ChangeAccess 'payamavar0\Enterprise Admins'
-ReadAccess 'payamavar0\Domain Users'
```

نکته: به صورت پیشفرض، سوییچ FolderEnumerationMode بر روی گزینه ی نامحدود قرار دارد.

- اگر Shared Name یک فایل درون سیستم را داشته باشیم و آدرس دقیق آنرا بخواهیم:

```
Get-SmbShare -Name cmts
```

- برای مشاهده ی Share Permission های به یک فایل، توسط shared Name آن:

```
Get-SmbShareAccess -Name cmts
```

- برای افزودن یک Permission خاص به یک فایل Share شده:

```
Grant-SmbShareAccess -Name cmts -AccessRight Full -AccountName 'payamavar0\Domain Controllers'
-Force
```

- برای سلب یک Permission از یک فایل Share شده:

```
Revoke-SmbShareAccess -Name cmts -AccountName 'payamavar0\payam1' -Force
```

- برای deny یا عدم آن، جهت دسترسی یک کاربر یا گروه به یک Shared File:

```
Block-SmbShareAccess -Name cmts -AccountName 'payamavar0\domain users' -Force
Unblock-SmbShareAccess -Name cmts -AccountName 'payamavar0\domain users' -Force
```

هربار که یک سیستم به فایل های Share شده ی سیستم ما متصل می شود، یک Session برقرار می شود.

- برای مشاهده ی Session های برقرار شده:

```
Get-SmbSession
```

- برای بستن همه ی Session های برقرار شده:

```
Close-SmbSession
```

- برای بستن یکی از Session ها:

```
Close-SmbSession -ClientComputerName 192.168.139.150
```

در حقیقت در هر سیستم ویندوزی، پروتکل SMB وجود دارد، که به نام SMB Server شناخته شده و شامل دو ورژن 1 و 2 می باشد. به دلایل امنیتی، ورژن قدیمی تر، یعنی یک را، غیرفعال می کنیم.

- برای مشاهده ی تنظیمات SMB Server هر سیستم:

```
Get-SmbServerConfiguration
```

- برای غیرفعال کردن ورژن 1 آن:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- می توان قابلیت حسابرسی و گزارش گیری را فعال کرد:

```
Set-SmbServerConfiguration -AuditSmb1Access $true
```

همچنین می توان تنظیمات SMB را برای Client ها هم در خود سیستم Server مشاهده کرده و تغییر دهیم:

```
Get-SmbClientConfiguration
```

: NTFS Permission

مجوزهای NTFS فقط بر روی فایل ها یا پوشه هایی که درون Partition های NTFS هستند، اعمال می شوند.
وقتی برای یک فایل، مجوزهای NTFS، تعریف می کنیم، این مجوزها به آنها پیوست شده و در صورت تغییر یا جابجایی فایل ها از درایوی به درایو دیگر، همراه با فایل خواهند بود.

- این مجوزها با فایل ها می مانند تا زمانی که جابجایی، از یک درایو NTFS به یک درایو NTFS یا ReFS دیگر باشد.

پس وارد Server Manager و بخش Shares از File and Storage Services شده و به Properties فایل Share شده و تب Permissions رفته و Customize permissions را می زنیم.

تعریف NTFS Permission، به دو صورت قابل انجام است:

- **: Basic**

  در بخش بالایی، بر روی Edit می زنیم.
- **: Advanced**

  در بخش پایینی، بر روی Advanced می زنیم.
- در پنجره ی باز شده، تب Permissions مربوط به NTFS Permissions و تب Share مربوط به Share Permissions است.

نکته:
بجای استفاده از Share Permission ها، از NTFS Permission ها استفاده می کنیم، چون ساده تر پیاده سازی می شوند و همیشه همراه فایل خواهند بود.
پس در پنجره ی Advanced و تب Share، فقط برای Everyone ، نوع Allow را همراه با Access ای در حالت Full Control قرار می دهیم.

- NTFS Permission مربوط به یک فایل، شامل یک ACL (Access Control List) می باشد.
  ACL یک لیست است که مشخص می کند چه کسانی به این فایل، دسترسی داشته باشند و چه کسانی نداشته باشند.
  - این ACL، همان لیستی است که در پنجره ی Advanced و تب Permissions می بینیم.
  - ACL شامل تعدادی ACE (Access Control Entry) می باشد، که همان گزینه های تعیین شده برای ACL می باشند.

- برای همه ی فایل ها و پوشه های (Child ها) درون یک پوشه ی دارای NTFS Permission نیز، آن Permission ها را دریافت کنند، می توانیم قابلیت Inheritage را برای ACE ها تعریف کنیم.
  - پس Inheritage را می توان به زیرمجموعه ها (Child ها) هم به ارث رساند. (ستون Applies to مربوط به ACE ها)
  - Inheritage می تواند از کسی یا جایی به ارث برده شود و یا اینکه نشود. (ستون Inherited From مربوط به ACE ها)

- جهت تعریف ACE، بر روی دکمه ی Add کلیک کرده و سپس بر روی Select a Principal زده و یک کاربر یا گروه را اضافه می کنیم.
  - حال توسط گزینه ی Applies to می توانیم تعیین کنیم که این مجوز، به چه شکل به ارث برسد.
  - در بخش basic Permissions می توان یک مجوزدهی کلی تعیین کرد؛ اما اگر در سمت راست، .Show advanced P را بزنیم، می توانیم مجوزدهی های جزیی تری را تعریف کنیم:
  - همه ی گزینه ها واضح اند، اما اگر کاربری دسترسی به یک فایل نداشته باشد، پس نخواهیم که بتوانند آن را اجرا هم بکنند، گزینه ی Traverse Folder را غیرفعال می کنیم.

نکته: حال برای اینکه Inheritage بکار بیفتد، باید در پایین پنجره ی Advanced، گزینه ی Enable Inheritage هم فعال باشد.
نکته: فرض کنید که برای Domain User ها قابلیت read را فعال کرده باشیم، یا اینکه هر قابلیت را، به جز Create فایل را فعال کرده باشیم.
اما خواهیم دید که Domain User ها با ورود به فایل Share شده، می توانند پوشه ی جدید هم ایجاد کنند!

این به دلیل قابلیت **Inheritage** است که ویژگی **Create File** را از پوشه های بالادستی، به ارث برده اند.
برای اینکه این قابلیت های موردنظر را برای **Domain User** ها قطع کنیم، به همان شکل، **Add** را زده و **Domain Users** را وارد می کنیم، اما به جای **Allow**، آن را در حالت **Deny** قرار داده و دو گزینه ی **Create Files** و **Create Folders** را تیک می زنیم.

تذکر: احتمالاً برای اعمال برخی تغییرات، باید یکبار Sign out کرده و دوباره sign in کنیم.

Effective Access :

برای اینکه بدانید، یک **User** و یا اعضای یک **Group**،
در یکی از سیستم های شبکه، چه **Permission** هایی دارند:
در پنجره ی **Advanced Security** وارد تب **Effective Access** شده و در برابر **User/Group**، آن **User** یا **Group** را وارد می کنیم؛
سپس در برابر **Device**، سیستم موردنظر را وارد کرده و در پایان روی **View effective access** کلیک می کنیم.

Fast Working on Users :

Net User :

یکی از دستورهای قدیمی در **CMD** که باعث افزایش سرعت عمل یک **Admin** شبکه می شود، دستور **net user** است که فقط با حساب **Administrator** عمل می کند!

اگر این دستور را به تنهایی وارد کنیم، ابتدا نام **PC** را نمایش می دهد، سپس تمام **User** های موجود در سیستم یا شبکه را لیست می کند.

net user

ایجاد یک **User** :

Net user نام یک پسورد یک /add /domain

Net user ali 123456 /add /domain

نکته: این دستور را که می توان با **net user** وارد کرد را، می توان در خط فرمان **RUN** هم وارد کرد و فوراً عمل خواهد کرد!

- اگر بخواهیم پسورد را به شکل رمزی و نامحسوس وارد کنیم، به جای پسورد، علامت * را درج می کنیم.
- **User** های از این طریق ایجاد شده، وارد کانتینر **Users** می شوند.

نکته: پس هرگاه که مدیر حتی برای زمانی کوتاه پشت سیستم نیست، باید سیستم را **Lock** کند، چون به سادگی و به سرعت هرکسی می تواند آمده و به هر قصدی، یک **User** بسازد.

ایجاد یک **User** با تاریخ انقضا: مثلاً سیزدهم **August** سال **2020** :

net user ali 123456 /add /domain /expires:08/13/2020

به این معنی که این حساب تا پایان روز دوازدهم **August** فعال خواهد ماند.

ایجاد یک **User** با تعیین اینکه از کدام کامپیوترها قابل ورود باشد:

net user ali 123456 /add /domain /workstations:pc1,pc2

مشاهده ی مشخصات مهم و اساسی مربوط به یک **User** :

Net user نامUser

فرض کنید تنها حساب کاربری که با آن وارد **PC** می شدید، **disable** شده است!

برای فعال سازی حساب کاربری سیستم اصلی:

DVD ویندوز را در کامپیوتر قرار داده و از طریق آن کامپیوتر را **Boot** می کنیم.سپس **Shift+F10** را می زنیم تا **CMD** باز شود:

net user ali /active:yes

برای حذف یک حساب کاربری:

net user ali /delete

: Net Account

اگر این دستور را به همین صورت (**net account**) وارد کنیم، همه ی قابلیت های ممکن را که توسط جایگذاری هریک از کلماتی که لیست شده اند، به جای کلمه ی **account**، نشان خواهد داد.

- **Net accounts** : تنظیمات **Password Policy** را خواهیم دید.

: Net use

این دستور دو کاربرد دارد:

- برای ایجاد یک **map drive** از یک پوشه ی **share** شده در شبکه
- برای اضافه کردن یک **Printer** عضو شبکه به لیست **Printer** های سیستم جاری

مثلاً **map drive** از پوشه ی **music** از کامپیوتر **Server01**:

Net Use * "\\Server01\music"

- علامت ستاره، به این معنی است که اولین حرف آزاد برای درایوها را، بطورخودکار به این **map drive** اختصاص بده.
- درصورت درنظر داشتن یک حرف خاص:

Net Use F: "\\Server01\music"

- بطورپیشفرض، این **map drive** یکبارمصرف خواهد، بود یعنی پس از یکبار **restart** از بین خواهد رفت، مگراینکه:

Net Use F: "\\Server01\music" /persistent:yes

یا

Net Use F: "\\Server01\music" /p:yes

- اگر کامپیوتر **Server01** دسترسی را تنها توسط وارد کردن یک حساب مجاز محدود کرده باشد، پس از اینکه سیستم را یکبار **restart** کنیم و سعی به دسترسی بر این **map drive** داشته باشیم، دوباره نیاز به وارد کردن مشخصات **credential** خواهد بود، مگر:

Net Use F: "\\Server01\music" /PASSWORD /User:USERNAME /p:yes /savecred

- اگر پوشه ی مقصد در **Server01**، عضوی از همین شبکه ی جاری باشد، بهتر است که عبارت **/home** را نیز به پایان اضافه کنیم:

Net Use F: "\\Server01\music" /PASSWORD /User:USERNAME /p:yes /savecred /home

- برای حذف یک **map drive**، تنها نام آن نیاز خواهد بود:

Net Use F: /delete

مثلاً افزودن پرینتر با نام **Epson_01** از سیستم **Server02** به لیست **Printer** های سیستم جاری:

Net Use LPTx "\\Server02\Epson_02" /persistent:yes

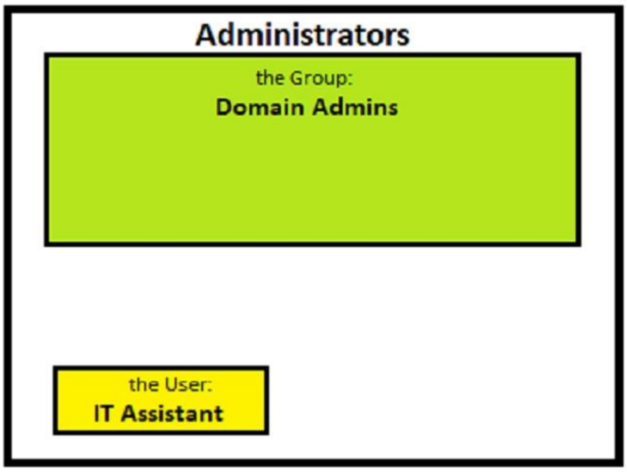
:Admin permissions for Assistants

در شبکه های بزرگ، که مدیرشبکه، دستیار یا دستیارهایی هم خواهد داشت، لازم است که این دستیارها، بر روی تمام کامپیوترهای Client ها، تمامی حقوق Administrator را داشته باشند. پس لازم است که Account آنها نیز، عضو گروه Domain Admins شود.

اما از طرفی، اعضای گروه Domain Admins، قادر به دسترسی به Server ها و اعمال تغییرات بر روی آنها خواهند بود.

پس راه حل مطمین و امن، به این صورت است که وارد هریک از کامپیوترهای Client ها شده و Account دستیارهای شبکه را، یکی یکی عضو گروه Administrator که به صورت محلی روی آن کامپیوتر است، کنیم.

نکته: خود گروه Domain Admins بطورپیشفرض (پس از join شدن یک کامپیوتر به Domain) عضو گروه local Administrator خواهد شد.



اما از آنجایی که تعداد کامپیوترهای Client در شبکه های بزرگ زیاد بوده و اعمال این عضویت بر روی همه ی آنها، منطقی نیست، پس:

روش اول: به کمک یک GPO، یک اسکریپت کوتاه، جهت عضو کردن حساب Assistant در local administrator را به شکل یک فایل bat تعریف می کنیم و به OU مربوط به همه ی کامپیوترهای Client ها، اختصاص می دهیم.

مثلاً عضو کردن حساب Ali1 در شبکه ی payamavar:

Net Localgroup Administrators “payamavar\Ali1” /add

روش اول: یک GPO ایجاد کرده و وارد تنظیمات آن شده و به مسیر زیر می رویم:

Configuration/Windows Settings/Security Settings/Restricted Groups

بر روی اون راست کلیک کرده و گزینه ی Add Group را می زنیم.

در این قسمت نام گروه local را، (در اینجا Administrators) وارد می کنیم. (از Browse استفاده نمی کنیم.)

می توانیم در ادامه، گروه های دیگری که می خواهیم به عنوان Local Administrators در Client ها عضو شوند را نیز وارد می کنیم.

نکته: در Active Directory بصورت پیشفرض گروه های Domain Admins و Enterprise Admins به عضویت Local Administrators در آمده اند. اما به محض اعمال Policy بالا، تمامی گروه ها و کاربرهایی که در این گروه قرار گرفته اند، به عنوان Local Administrator شناخته شده و سایرین از گروه، حذف می شوند.

پس همیشه گروه های Domain Admins و Enterprise Administrators را به Restricted Group اضافه می کنیم.

حال این GPO را به OU مربوط به همه ی کامپیوترهای Client ها، اختصاص می دهیم.

Additional DC (ADC) :

همانطور که می دانیم در هر شبکه می توان بیش از یک Domain داشت.

- یا با یک نقش و وظایف خاص خودش.
- یا به عنوان یک Support Domain (Standby Domain) به جهت Redundancy یا همان High Availability و افزایش سرعت Authentication و ... .

مثلاً وقتی داده ای در یکی از Domain ها دچار تغییر می شود، بسته به اهمیت آن در شبکه، یا فوری و یا بعد از گذشت زمانی، از چند دقیقه تا چند ساعت، در تمام Domain های دیگر Replicate می شود.

وقتی یک شبکه دارای Site هایی با فواصل جغرافیایی زیاد از هم باشد، به جهت نیاز به سرعت بالا برای Authentication و Authorisation در همه ی Site ها، عاقلانه ترین کار این است که در هر Site یک Domain Controller مختص خودش قرار دهیم که بطور معمول از طریق WAN Link به Domain Controller اصلی متصل می شوند.

انواع Additional DC :

- Writable DC : حالت پیشفرض است.
  در این حالت Additional DC هم می تواند اطلاعات و تنظیمات AD را Edit کند. مثلاً ایجاد یا حذف user ، Group ، OU و ...

- Read-only DC :
  این نوع Additional DC تنها دسترسی خواندنی به اطلاعات و تنظیمات AD دارد و تقریباً قادر به هیچ تغییری نیست.

:an Additional Domain deployment

پس درست مثل ایجاد اولین Domain عمل می کنیم.

1. ویندوز Server را نصب می کنیم.
2. تمام پیشنیازهای اولیه ی مشترک بین همه ی System ها را برای آن انجام می دهیم.
3. در Control Panel و System، آن را عضو Domain می کنیم.

اگر نسخه ی Server Core بود، به یکی از دو روش زیر آن را عضو Domain می کنیم:

تحت CMD	Netdom join %computername% /domain: Payamavar.local /userd: administrator /password:XX
تحت PowerShell	Add-Computer -DomainName payamavar.local

پس از دستور PowerShell اطلاعات یک User مدیر از Domain اصلی شبکه را می خواهد که نام را بصورت زیر درج می کنیم:
Administrator@payamavar.local

به یکبار Restart نیاز خواهیم داشت.

4. **AD DS Role و DNS Role را نصب می کنیم.**

- شروع به نصب DC می کنیم.
- در صفحه ی نصب DC، اولین گزینه یعنی **Add a Domain Controller to an existing Domain** را زده و نام **Root Domain** را وارد کرده و ادامه!
- با **IFM** کاری نداریم، اما برای **Replicate from**، گزینه ی **Server** را انتخاب کرده و می رویم برای نصب.

5. **تغییرات لازم را اعمال می کنیم.**

وقتی نصب تمام شد، اولین بار با حساب **Domain Administrator** وارد شده و اگر تنظیم خاصی لازم باشد، انجام می دهیم.

نکته:

اگرچه این Domain، از نوع **Read and Write DC** می باشد، اما قادر و مجاز نیست که دقیقاً و 100٪ مثل **main Domain**، در تنظیمات شبکه، تغییر ایجاد کند!

اولاً در تمام شبکه، فقط با حساب Administrator مربوط به main Domain می توان همه ی دسترسی ها را داشت و هرکاری انجام داد.
اما از طرف دیگر، برخی کارها هستند که نه تنها فقط با حساب Administrator، بلکه فقط در خود سیستم Domain، امکان پذیر هستند!

- ❖ وقتی تغییری در **Service** ها یا **Site** ها و یا در **DNS** و یا در **DHCP** می دهیم، برای اینکه فوری موثر واقع شود، می توان در **cmd** دستور **repadmin /syncall** را وارد کرد.

- ❖ در حقیقت وقتی **replicate** انجام می شود، پوشه ی **Sysvol** که در درایو **C** و پوشه ی **Windows** سیستم **Server** اصلی شبکه قرار دارد، **Update** می شود.

برای دستیابی به این پوشه در تمام شبکه، می توان در Win.Explorer درج کرد:

\\نام کامپیوتر دامین کنترلر

: Repadmin

Windows Server شامل یک command است که می تواند برای تشخیص خطا در عملیات Replication به ما کمک کند و آن repadmin می باشد.
اولین ابزار در رابطه با دستور repadmin، دستور replsummary است که خلاصه ای از سلامت Replication جاری را به ما نشان می دهد:

repadmin /replsummary

: Global Catalog

هر DC یک کپی از همه ی Object های درون Forest را در اختیار دارد.
Global Catalog یک کپی read-only از همه ی آبجکت های Forest و صفات آنها می باشد.
در واقع قابلیت جستجو در همه ی AD DS های همه ی Domain های موجود در Forest را فراهم می سازد و بیشترین کاربرد را برای انجام جستجوها در ساختارهای Multi-domain که در آنها جستجوی Object ها به کندی انجام می شود را دارد.
باعث می شود که درهنگام join شدن Client ها به Domain، به سهولت main DC و منابع شبکه را بیابند.

- Global Catalog اطلاعات object های Domain خودش را به صورت کامل و اطلاعات object های Domain های دیگر را به صورت کلی و در حد Attribute دارد.
- Global Catalog اطلاعات تمام Forest را در هنگام Replication بین DC ها دریافت می کند.

مثلاً اینکه هریک از اکانت ها عضو چه گروههایی هستند و ...، درون این کاتالوگ ذخیره می شوند.
این کاتالوگ روی اولین DC بصورت خودکارفعال است، اما مدیر شبکه تعیین می کند که روی کدامیک از سایر DC ها نصب شود یا نشود.

اگر DC اول کنار برود وکاتالوگ فوق روی سایر DC ها نصب نشده باشد، مشکلات زیادی بوجود خواهد آمد:

- دیگرهیچ کاربری نمی تواند به دامین Log on شود.
- حتی اعضای domain admins ازآن پس فقط بصورت Interactive (برحسب شناخت دوطرفه) و فقط به خودِ DC می توانند Logon کنند، چون رابطه ای بین کلاینت ها و DC ها پیدا نمی شود.
- همچنین search و Detection در DC بسیار ضعیف می شود.

اگر درکنسول active directory Sites and services در پنل سمت چپ،کشوی Sites و سپس کشوی مربوط به نام Site را باز کنیم، در فولدری به نام Servers ، همه ی DC های Forest قابل مشاهده اند.اگر جلوی نام یک DC و زیر ستون DC type کلمه GC نوشته شده باشد به این معناست که روی DC فوق گلوبال کاتالوگ نصب می باشد.

برای غیرفعال سازی Global Catalog روی یک DC کافی ست در همان کنسول Active directory Sites and services روی NTDS settings راست کلیک کرده و با انتخاب گزینه properties و سپس در تب general ، چک باکس Global Catalog را غیرفعال کنیم.
جستجوهایی که به سمت Global Catalog Server ها هدایت می شوند، نسبت به سایر جستجوها سریعتر انجام می شوند.

Global Catalog یک نسخه ی سطحی و سبک از Directory Partition های تمام Forest است، چون تمامی خاصیت های آبجکتها در آن وجود ندارند و تنها برخی از Attribute ها در آن وجود دارند.
با متمرکز سازیِ Attribute های خاصِ Object ها، که صرفا برای جستجو و پیدا کردن آنها در شبکه مورد استفاده قرار می گیرند، می توان یک پایگاه داده ی کامل از همه ی آبجکت های موجود در تمام محیط Domain را در یک Global Catalog Server در اختیار داشت.
پس بیشترین و مهمترین کاربردGlobal Catalog ، جستجو و بازیابی Object ها در ابعاد Forest است.

نکته: در محیط های تک دامینی، در صورت بروز اشکال برای گلوبال کاتالوگ، مشکل چندانی وجود نخواهد داشت، اما در Multi-Domain Environment هاست که مشکل ساز خواهد شد.

از آنجاییکه اعضای گروه های Universal می توانند از چندین domain مختلف باشند، باید ساختاری وجود داشته باشد تا سیستم تشخیص دهد که کاربر موجود، در کدامیک از Domain های مجموعه عضویت دارد.
تنها DC ای که می تواند این مشکل را برطرف کند، آنDC ای است که دارای نقش Global Catalog است.
این DC، لیست تمامی گروه های Universal مربوط به Forest را به همراه اعضای آنها در اختیار دارد و به راحتی می تواند مشکل را حل کند.

می توان در کنسول AD Sites and Services در پنل سمت چپ، نام Site را انتخاب کرده و در سمت راست روی NTDS Site Settings راست کلیک کرده و properties را انتخاب کنید و در پنجره ی ظاهر شده، گزینه ی..Enable Universal Group Membership را فعال کنیم تا اگر کاربری با عضویت در یک گروه Universal Group به سیستم Login کرد، تنظیماتUniversal Group Membership مربوط به او، Cache شود تا login های بعدی او، سریعتر صورت پذیرند.
این عملیات Caching هر 8 ساعت یکبار بطور خودکار refresh می شود.

یکی دیگر از دلایلی که Multi-Domain Environment ها به Global Catalog نیاز دارند، ورود به سیستم از طریق ساختار UPN یا Universal Principal Name است، که به آن FQDN هم می گویند.
ساختار نامگذاری اسامی اعضا بصورت UPN، شبیه به ساختار ایمیل است: username@domainname

پس Global Catalog وظیفه ی بدست آوردن و شناسایی ساختارهای UPN را برای ورود هر کاربر به سیستم، بر عهده خواهد داشت.

نکته: یکی از سرویس هایی که نیاز زیادی به Global Catalog دارد، سرویس Exchange Server می باشد.

Read Only Domain Controller (RODC):

- RODC نوعی Server است که اطلاعات درون بانک داده ها و Domain Controller آن، فقط قابل خواندن باشند.
- این نوع سرور را معمولاً به عنوان یک سرور جانشین برای سرور اصلی که البته از نوع RWDC می باشد، استفاده می کنند.
- در حقیقت سرور RODC از طریق یک لینک (شبکه ی WAN یا شبکه LAN) با RWDC Server در ارتباط است.
- در حقیقت در لحظه ی اول Implementation یک RODC Server ، این سرور کاملاً خالی و فاقد اطلاعات است.

- از اولین درخواست هایی که از سوی کاربرها به سمت RODC می آید، بانک داده ی RODC شروع به پر شدن می کند.
- به این صورت که بعد از دریافت یک درخواست، متوجه می شود که در بانک خودش، اطلاعات مشابه با آن درخواست را ندارد،
- پس این درخواست را به سمت RWDC ارسال یا همان forward می کند.
- RWDC درخواست های RODC را بررسی می کند، و سپس در صورت موجود بودن داده های مرتبط با آن، پاسخ را به سوی RODC ارسال می کند.
- وقتی RODC پاسخ RWDC را دریافت می کند، علاوه بر ارسال آن پاسخ به کاربر درخواست کننده، آن پاسخ را در بانک داده ی فقط خواندنی خودش هم ذخیره می کند.یا به قولی این اطلاعات دریافتی را Cache می کند.
- این Cache کردن اطلاعات در صورتی انجام می شود که قابلیت «Cache کردن» در آن RODC فعال شده باشد.

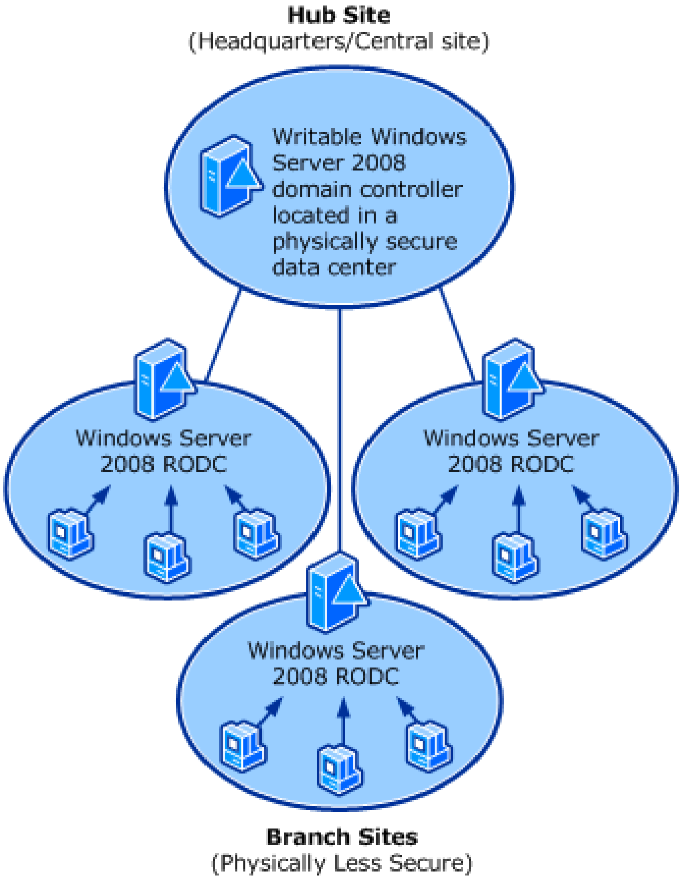
- از طرف دیگر، RWDC هم لیستی از اطلاعاتی که توسط RODC، Cache شده اند را نگهداری می کند.

به همین جهت، به طور مدام و البته یکطرفه از سمت RWDC به سوی RODC، به محض ایجاد تغییر در محتوای اطلاعاتی که روی RWDC قرار دارند و در RODC هم Cache شده اند، نسخه ی تغییریافته ی آن اطلاعات، برای RODC ارسال و جایگزین می شود.

از آنجایی که این Replication یا رونوشت یا همانندسازی، فقط یک طرفه صورت می گیرد، هیچ خطری شبکه را تهدید نمی کند و تنها کافیست که امنیت برای همان اطلاعات Cache شده، تأمین شود؛ مثلا Password های همان عده از کاربران یا اطلاعات Cache شده، update شوند، کافی ست.

فرض کنید لینک اتصال میان RODC و RWDC، اینترنت باشد، در نتیجه لینک اتصال میان این دو Server هنوز هم مستقیم نخواهد بود!
چرا که هیچگاه یک RWDC را بطور مستقیم به یک فضای عمومی مثل اینترنت وصل نمی کنیم. به سادگی هک خواهد شد!
پس در کنار RWDC، یک RODC راه اندازی می کنیم و آنها را به هم وصل می کنیم، و RODC راه دور را به RODC در کنار RWDC وصل می کنیم.

:Useage of RODC



معمولاً Branch Office ها یا شعبه های یک شرکت بزرگ، با شرایط محدود کننده ای مواجه هستند، مثل:

- پهنای باند کم،
- امنیت فیزیکی نا مناسب،
- عدم وجود تکنسین شبکه،
- تعداد کم کاربر
- و ...

پس نگه داشتن یک writable DC در آنها، ریسکی بزرگ است.

در گذشته راه حلی مناسب تر از راه اندازی یک DC در Branch Office نداشتیم، اما با ظهور ویندوز Server 2008 ، دامین کنترلرهای RODC معرفی شدند که راه گشای بسیاری از مشکلات گذشته بودند.

وجود قابلیت RODC می تواند هزینه های پیاده سازی و نگهداری را کم کند.

- توصیه می شود که در هر Domain حداکثر یک RODC وجود داشته باشد، حتی اگر این Domain دارای چندین Site باشد.
- اگر بیش از یک RODC در یک Domain موجود باشد، فرآیند log on کردن کاربران، دچار مشکلات زیادی می شود.

- اگر در Forest خود چند Domain داشته باشید، RoDC نمی تواند اطلاعات اکانتهای Domain های دیگر (غیر از دامین خودش) را Cache کند.

: Implementation of a RODC

برای راه اندازی یک RODC:

- ابتدا باید روی آن سیستم، یک ویندوز Server، بدون اتصال به Domain Controller اصلی، نصب کرد و یک نام مناسب در قسمت Computer Name برای آن درج کرد.
- وقتی کاملاً آماده و یکبار reset شد، با local Account Admin ، وارد سیستم می شویم.

نکته:

در ابتدای کار، نباید هیچگونه DC و یا Role دیگری روی سیستم در نظر گرفته شده بعنوان RODC نصب کرد و ترجیحاً بیشتر تنظیمات را به شکل Default رها می کنیم، به جز آدرس DNS آن، که در Network Adapter ، دقیقاً همان آدرس DNS شبکه ی اصلی را می دهیم.

باید این سیستم، قادر باشد به سیستم سرور اصلی Ping شده و جواب بدهد.

اتصال این سیستم RODC را به main Domain، بصورت Non-staged انجام می دهیم.

- نیاز است که یک User برای شخصی که بجای مدیر اصلی کل شبکه، با سیستم RODC کار می کند، ایجاد کنیم، پس در main Server وارد AD users and comuters می شویم، و یک User معمولی برای آن می سازیم.
- حال باید در سیستم اصلی، سیستم RODC را پیش ساخت کنیم.

پس در همین AD users and comuters، وارد پوشه ی Domain Controllers شده و با کلیک راست، گزینه ی Pre-Create Read Only Domain Controller account را می زنیم.

- Use Advanced mode را فعال می کنیم.
- نام کامپیوتر مقصد که نقش RODC را خواهد داشت، وارد می کنیم.
- DNS Server و Global Catalog را فعال می کنیم.
- پنجره ی Specify the Password replication policy در این مورد است که کدام پسوردها در سیستم RODC هم ذخیره و Update شوند؛ که بر طبق قاعده، ما نمی خواهیم که پسورد اپراتورهای معمول سرور را به کاربر یا سیستم RODC ارسال یا replicate کنیم، و فقط آخرین گروه، یعنی گزینه ی allowed RODC Password Replication group را در حالت allow نگه می داریم.

- در بخش ..Delegation of RODC Insta کاربر یا گروهی از کاربران را که برای کار با RODC Server تعیین کرده ایم را انتخاب می کنیم، که همان کاربری که اخیراً در Server ایجاد کردیم را انتخاب می کنیم و تمام!

پس تا اینجا سیستم RODC را در سرور اصلی ایجاد و ثبت کردیم، اما هنوز روشن نیست!

حال از شخصی که در شعبه و پشت سیستم است درخواست می کنیم که عملیات زیر را انجام دهد:

- در سیستم RODC باید، نقش Active directory Domain Services را نصب کنیم و در پایان، گزینه ی Promote this Server to a domain controller را زده و سپس گزینه ی Add a DC to an existing domain را انتخاب کرده و در قسمت نام Domain ، نام دامین سرور اصلی را وارد می کنیم.
- سپس با انتخاب next ، مشخصات user ای که در Server اصلی، برای <u>کاربر جانشین مدیر شبکه در بخش شعبه</u>، ایجاد کرده بودیم را وارد می کنیم. اما بصورت آدرس Domain :

نام یوزر \ نام دامین اصلی

- در ادامه، گزینه ی **use existing RODC Account** را زده و یک پسورد برای مواقع اضطراری درج می کنیم.
- برای **replicate from** ، نام **Domain** اصلی را انتخاب می کنیم.
- **Install** می کنیم.
- **Reset** می کند.
- حال با **User** ای که برای **RODC** تعریف کرده بودیم می توانیم وارد سیستم **RODC** شویم.

نکته: برای خیلی از عملیات، مثل **remove** کردن سرویس ها و **Role** های **AD** در این سیستم، تنها با دسترسی مدیر کل **Domain** می توان آنها را عملی کرد، در غیراینصورت، کاری از کاربر تعریف شده برای سیستم **RODC** بر نمی آید.

: Password Replication Policy (PRP)

PRP یک **Access Control List** است که مشخص می کند که مشخصات کدام **Account** ها و کدام **PC** ها می توانند در **RODC**، کش شوند.
اولاً به هیچ وجه نباید اجازه ی Cache شدن پسوردهای Administrator ها در RODC را داد.
دوماً فرض کنید هزاران کاربر در کل یک سازمان دارید، اما در یکی از **Branch Office** ها، فقط چند کاربر دارید، در این صورت **replicate** کردن رمز عبور همه ی کاربران کل سازمان، برای تمام کاربران **domain**، ایده ی مناسبی نیست.
به این منظور می توانیم امنیت را از طریق **replicate** نکردن رمز عبورهای کاربرانی که در آن اداره وجود ندارند، افزایش دهیم.

می توان گروههایی را تعیین کرد که فقط پسوردهای اعضای آنها در **RODC** کش شوند.
می توان گروههایی را تعیین کرد که پسوردهای اعضای آنها در **RODC** کش نشوند.

پس در کنسول **AD Users and Computers** و در **OU** مربوط به **Domain Controllers**، وارد **Properties** سیستم **RODC** می شویم.
در تب **Password Replication Policy** می توانیم تعیین کنیم که برای **cache** شدن در این **RODC** کدام گروه ها **Allow** و کدام گروه ها **Deny** باشند.

در همین تب، با ورود به دکمه ی **Advanced** می توان تشخیص داد که :

- تا بحال کدام **Account** ها **cache** یا **Store** شده اند،
- تا بحال با کدام **Account** ها **authenticate** و **Log in** انجام شده است.

همچنین می توان با **Prepopulate Passwords** برخی **Account** ها را از همان ابتدا **Cache** کرد.

نکته:
اگر در شعبه ای از **RODC** استفاده می کنید، وظیفه ی **Authenticate** کردن **User** های آن شعبه، برعهده ی خود سرور **RODC** می باشد، اما احراز هویت همه ی کامپیوترها توسط **main DC** انجام می شود، به این شکل که در هنگام **Login**، ابتدا کامپیوتر احراز هویت می شود و سپس **User**. پس اگر کامپیوترها توسط **DC** اصلی احراز هویت نشوند، احراز هویت شدن **User** ها توسط **RODC** ممکن نیست!

نکته: بهتر است که **RODC** را روی بستر **Virtual** ایجاد کنیم و هارد فیزیکی آن را با **bitlocker** رمزنگاری کنیم که اگر هارد فوق به سرقت رفت، قابل استفاده نباشد.

اگر در شبکه دارای چندین **Site** باشیم و بخواهیم در آنها **RoDC** کنیم، در مورد **Password Replication Policy** بهتر است از گروه **Allowd RODC Password Replication** استفاده نکنیم، چون اکانتهایی که برای یک **Site** مجازند با اکانتهای مجاز برای سایت دیگر فرق دارند. پس در چنین مواقعی برای هر **RODC** صرفاً گروههای مجاز را **Allow** می کنیم و برای هر **RODC** گروه مخصوصی ایجاد می کنیم.

: IFM (Install From Media)

همانطور که می دانید برای راه اندازی یک Additional DC نیاز است که به Database مربوط به Active Directory اصلی و همچنین به پوشه ی Sysvol و تنظیمات Registry که در Root Domain Controller موجود هستند، دسترسی داشته باشیم.

اگر به صورت معمول به نصب این ADC بپردازیم، لازم است که در حین نصب، ارتباط شبکه ای مناسبی با RootDC مورد نظر داشته باشیم تا Data مورد نیاز، به سمت ADC منتقل شده و نصب انجام پذیرد.
حال اگر ارتباط شبکه ای بین main Domain Controller و ADC دچار قطعی های مکرر یا مشکل پهنای باند باشد، از آنجایی که این Data ی مورد نیاز که باید از سمت Server به ADC ارسال شود، حجم بالایی دارد، کار آنچنان هوشمندانه ای نیست.

در این روش، ابتدا از RootDC یک Backup از نوع IFM تهیه می کنیم و سپس این Backup را که تحت یک رسانه ی ذخیره سازی مثل CD ، DVD و یا USB Memory به سرور ADC منتقل می کنیم و در مراحل نصب DC، این پوشه را به عنوان Source جهت معرفی Database و Sysvol معرفی می کنیم.

از آنجایی که فایل Database مربوط به Active Directory شبکه ، NTDS نام دارد، باید کمی در مورد آن بدانیم.
NTDS فایلی است با پسوند dit، که یک Domain Controller داده های AD را در آن ذخیره می کند.

در فایلNTDS.DIT ، اطلاعات در دسته بندی های مختلفی ذخیره می شوند:

1. Schema information : تمام جزئیات در مورد Object ها و Attribute های موجود در AD را درون خود دارد.این اطلاعات در تمام یکForest ، توسط DC ای که صاحب نقش Schema Master است، کنترل و دچار تغییر می شوند.

2. Configuration information : تمام جزئیات در مورد Forest و Tree را درون خود دارد.این اطلاعات در تمام یک Forest، توسط DC ای که صاحب نقش Domain Naming Master است، کنترل و دچار تغییر می شوند.

3. Application : اطلاعات این بخش در دو دسته قرار دارند:

- ForestDNSZones : درون آن رکوردهای SRV و CNAME مربوط به Forest ذخیره می شوند که توسط عملیات Replication، بین تمام DC هایی که دارای سرور DNS هستند، منتقل می شوند.

- DomainDNSZone : درون آن تمام رکوردهای DNS مربوط به Domain Zone ذخیره می شوند که توسط عملیات Replication بین تمام DC های موجود در یک Domain که دارای سرور DNS هستند، منتقل می شوند.

4. یک Database بر اساس ESE (Extensible Storage Engine) است، که دارای سه Table می باشد: Schema ، Link و Data.

برای تهیه ی Backup جهت IFM، وارد main RootDC شده و CMD را بصورت run as administrator باز می کنیم.

1. ابتدا باید وارد تنظیمات ntds شویم، پس تایپ می کنیم: **ntdsutil**
2. حال باید Instance یا درگاه تقاضا و درخواست را برای آن فعال کنیم: **activate instance ntds**
3. حال می توانیم IFM را فراخوانی کنیم، درج می کنیم: **ifm**
4. حال باید بدانیم برای کار با ifm، چه دستورهایی را و چطور باید وارد کنیم، پس برای راهنمایی، درج می کنیم: **?**
5. حال برای دریافت یک Backup کامل از یک RWDC، می توان از اولین دستور، همراه با یک آدرس دلخواه در خود سیستم استفاده کرد: **Create Full C:\New Folder**
6. پس از چند لحظه که تمام شد، دو بار **quit** را زده و اینتر، و کاملاً از محیط های IFM و ntds خارج می شویم و تمام!
7. حال باید پوشه ی ایجاد شده را توسط یک رسانه ی ذخیره سازی، به Server جدید منتقل کرد و AD DS را نصب کرد.

از قبل یک Computer Name مناسب برای DC جدید درج می کنیم.

حال در Server Manager آن، Role های AD DS و DNS را نصب می کنیم.

سپس اقدام به deploy کردن DC می کنیم:

- کاملاً مشابه نصب معمولی یک Additional DC است.
- گزینه ی Add a domain controller to an existing domain را انتخاب کرده و نام domain را درج می کنیم.
- فقط باید مواظب بود که گزینه ی RODC را فعال نکنیم!
- و در تب مربوط به IFM، تیک آن را فعال کرده و سپس فایل IFM ای که در main Domain ایجاد کرده بودیم و آورده ایم را انتخاب کرده و در زیر، نام Root Domain را انتخاب کرده و ادامه ی نصب را انجام می دهیم.

Clone a Domain Controller :

فرض کنید قصد داشته باشیم از یک DC یا یک Server مجازی، یک Clone تهیه کنیم. (چه در Vmware چه در HyperV و ...)
پس باید قبل از اقدام به Clone، یک سری تغییرات را بر روی DC موردنظر انجام دهیم که وقتی نسخه ی Clone را بالا می آوریم، به عنوان یک سیستم جدید بالا بیاید و نه اینکه با تمام مشخصات سیستم DC قبلی!

1. ابتدا باید این Domain را عضو گروه Cloneable Domain Controllers کنیم.

- پس در پنجره ی AD Users and Computers وارد OU ی Domain Controllers شده و روی Domain مورد نظر کلیک راست کرده و Add to a Group و ... .
- در حقیقت Clone گرفتن از یک سیستم، به این معنی است که سیستم مبدا را بدون هیچ تغییری، کاملاً کپی کنیم.
- در نتیجه، وقتی که هر دو سیستم روشن شوند:
- یک سری تغییرات ناخواسته مثل تخصیص IP و Name هماهنگ نشده اتفاق می افتد؛
- و احتمالاً یک سری Service ها یا Application ها که بر روی سیستم مبدا بوده است را بر روی سیستم جدید نیاز نخواهیم داشت.

2. پس نیاز است که ابتدا Serviceها یا Application های روی DC مبداء را exclude کنیم که از فرآیند clone گیری مستثنی شوند!

- وارد PowerShell ISE می شویم و دستور مقابل را درج کرده و Run می کنیم تا لیست سرویس ها بیایند:

```
Get-ADDCCloningExcludedApplicationList
```

- پس باید یک لیست از این Service ها یا App هایی که مستثنی خواهند شد به شکل یک فایل XML تشکیل داد و در درایو C و پوشه ی Windows و در پوشه ی NTDS ذخیره کرد. پس دستور بالا را یکبار دیگر، اما به شکل زیر درج و اجرا می کنیم:

```
Get-ADDCCloningExcludedApplicationList -GenerateXml -Path c:\windows\ntds -Force
```

3. حال باید شرایط یا تنظیمات دلخواهمان برای Clone کردن Active Directory را اعمال کنیم.

- پس در سمت راست Powershell ISE، دستور new-addccloneConfigFile را پیدا کرده و وارد زیرگزینه های آن می شویم.
- به تب Ipv4StaticSetting وارد شده و به جز Alternative Win Server و Preffered Win Server همه ی Field ها را پر می کنیم و تیک Static هم می زنیم. (یک IP و آدرس DNS و ...)
- برای Path هم، همان آدرس c:\windows\ntds را وارد کرده و در پایان، روی Run می زنیم.
- سیستم را خاموش کرده و از آن یک Clone می گیریم.
- اگر در Vmware باشیم، تنها کافی ست که از VM این DC، یک Clone بگیریم.
- اگر در Hyper-V باشیم که برای Clone گرفتن، باید آن را یکبار Export کرده و در پایان به شکل Create a new ID آن را Import کنیم.
- بهرحال پس از ایجاد Clone و راه اندازی سیستم clone شده، سیستم بطورخودکار به مسیر فایلی که در پوشه ی NTDS ذخیره شده بوده است می رود و از روی آن تنظیمات را انجام می دهد.

نکته:

قابلیت های Cloning، Pausing و Snapshotting باعث افزایش توانایی VMها می شوند، اما استفاده از هر یک از این قابلیت ها برای یک DC هرگز توصیه نمی شود.
مثلاً بازگشت به یک Snapshot از ماشین مجازی DC باعث می شود که Server و Database آن به حالت قبل برگردند که این حالت هرگز در طراحی Replication در نظر گرفته نشده است.کاربرهایی که Account آنها Delete شده، ممکن است هنوز بتوانند LogOn کنند و یا Account هایی که جدیداً ساخته شده اند، ممکن است با خطاهای غیر قابل پیش بینی مواجه شوند!
و یا پس از انجام Clone و استفاده از Clone، وقتی که DC متوجه می شود که Signature دیسکش تغییر کرده، خودش را از عملیات Replication جدا می کند! DC ممکن است کارش را ادامه دهد اما DC های دیگر با آن Replicate انجام نمی دهند!

Create a Child Domain :

1. روی سیستم مورد نظر یک **Windows Server** نصب می کنیم.
2. تنظیمات اولیه ی یک سیستم **Server** را روی آن انجام می دهیم.
3. این **PC** را به هر شکل ممکنی (VPN یا ...) به شبکه ی اصلی وصل می کنیم.
4. **DNS** و همچنین **Default Gateway** مربوط به **Root Domain** را برای آن تنظیم می کنیم.
5. **IP** سیستم را بصورت **Manual** تنظیم می کنیم.
6. یک **Name** برای این **PC** تعیین می کنیم و **Reastart**!
7. در **Server Manager** نقش های **AD DS** و **DNS** را نصب می کنیم.
8. دوباره وارد **System** شده و اینبار نوع شبکه را به **Domain** تغییر داده و نام **Root Domain** را درج کرده و **Reastart**.
9. با یک **Account** مدیر یا **Admin** در **Root Domain**، وارد می شویم.
10. گزینه ی **Add a new Domain to an existing Forest** را انتخاب می کنیم.
11. برای نام **Parent** ، نام **Root Domain** را و برای **new Domain**، یک نام برای **DC** اصلیِ این شبکه ی جدید که باید متفاوت با نام خودِ این **PC** که در آن قرار داریم، باشد.
12. بقیه ی مراحل را تا پایان به سادگی پیش می رویم.

(هرکجا که نیاز به معرفیِ یک **User** بود، همان **User** مدیری که با آن **Login** کرده ایم باید باشد.)

نکته: برای دسترسی به کنسول Active Directory Users and Computers مربوط به هر یک از Child Domain ها در سیستم Root Domain، کافی ست کنسول Active Directory Domains and Trusts را باز کنیم و در کادر سمت چپ، Child DC موردنظر را پیدا کرده و کلیک راست کرده و Manage را بزنیم.

Make the DC Offline :

نکته : اگر در شبکه، تنها یک DC داشته باشیم، اصلاً منطقی نیست که DC را Offline کنیم.
در حقیقت حداقل باید دو Additional DC در کنار main DC داشته باشیم.

روش اول:

باید سرویس AD DS را Stop کنیم.
پس وارد کنسول Services شده و Active Directory Domain Services را پیدا کرده و Stop می کنیم.
برای فعال کردن دوباره ی آن، روی آن کلیک راست کرده و Start را می زنیم.

روش دوم:

در این روش نیاز است که با یک Start up mode دیگر، وارد سیستم عامل شویم.
در سیستم های قدیمی تر، می توان یکبار سیستم را restart کرد و با فشردن دکمه ی F8 و یا Shift+F8 در هنگام Boot، گزینه ی Safe Mode را انتخاب کرده و وارد سیستم عامل شد.
اما در سیستم های UEFI و یا سیستم هایی که سیستم عامل شان بر روی SSD نصب شده است، نمی توان به این شکل وارد تنظیمات Start up Mode شد. پس در خود سیستم عامل ویندوز:

- ابتدا پنجره ی System Configuration را باز می کنیم. (در Run درج می کنیم: msconfig)
- در تب Boot گزینه ی Safe Boot و سپس AD repair را فعال و Apply می کنیم.
- سپس در تب General می بینیم که Selective Startup انتخاب شده است، کافی ست که از زیرگزینه های آن، فقط گزینه ی load startup items را فعال کنیم. OK می کنیم و Restart.

نکته: وقتی دوباره AD را به حالت اول برمی گردانیم، لازم است که پنجره ی Services را باز کرده و تمام سرویس هایی که نوع Startup آنها بر روی Automatic قرار دارند را Run کنیم، وگرنه DC در برخی عملیات مثل Replication دچار مشکل خواهد شد.

روش سوم:

در ویندوز، دکمه ی Shift را نگه داشته و کاملاً عادی در منوی Start ، بر روی دکمه ی Restart کلیک کرده و در ادامه مسیر زیر را طی می کنیم:

Troubleshoot > Advanced Options > Startup Settings > Restart

روش چهارم:

در این روش از طریق CMD و با دستور bcdEdit تعیین می کنیم که سیستم در حالت Safe Mode و با وضعیت DSRM وارد شود.
پس در cmd درج می کنیم:

```
bcdedit /set safeboot dsrepair
```

حال لازم است که یکبار سیستم را restart کنیم، درج می کنیم:

```
shutdown -r
```

برای بازگردانی سیستم به حالت قبل، دوباره CMD را باز کرده و درج می کنیم:

```
Bcdedit /deletevalue safeboot
```

```
shutdown -r
```

AD Defragmentation :

وقتی در یک سازمان، User ها و Computer های زیادی وجود داشته باشد، ارتباطات زیادی در هر روز با AD برقرار خواهد شد.
در نتیجه Active Directory و Database آن یعنی NTDS، خیلی زود fragment یا خرد و قطعه قطعه می شوند!
یعنی هم junk Data ها و هم فضای خالی غیرقابل استفاده ی AD زیاد خواهند شد.

پس لازم است که هرازگاهی Database مربوط به AD را Defragment کنیم که به نوعی Database را repair و البته Compact (فشرده) می کند.
در حقیقت اگر درحالت معمول و Online سیستم AD را Defrag کنیم، معمولاً بخوبی از عهده ی این کار برنخواهد آمد.
به همین جهت بطور ترجیحی، ابتدا AD را Offline می کنیم و سپس CMD را باز می کنیم:

1. Ntdsutil
2. Activate instance ntds

برای تعیین اینکه عملیات بر روی چه چیزی انجام شود:

3. Files

برای انجام عملیات Defragmentation :

4. compact to یک آدرس

مثلا : compact to c:\

برای چک و بررسی صحت عملیات انجام شده :

5. integrity
6. quit
7. quit

حال که عملیات Defragmentation انجام و نتیجه ی آن ذخیره شده است، باید این نتیجه ی ذخیره شده را جایگزین یا overwrite بر روی Database قبلی کنیم.
فایل NTDS جدید را از جایی که ایجاد شده است، برداشته و به جایی که بصورت default هنگام نصب AD DS تعیین کرده بودیم، ارسال می کنیم. پس در cmd درج می کنیم:

1. copy c:\ntds.dit c:\windows\ntds\ntds.dit
2. yes

در حقیقت بخشی از فایل های junk data که در database ایجاد می شوند، در همان پوشه ی NTDS و گزارش هایی با پسوند log. هستند که می توانیم همه ی آنها را حذف کنیم.

3. del c:\windows\ntds*.log

Group Policy :

ساختاری است که برای اعمال مجموعه ای از تنظیمات یا سیاست ها (Security or non-security) به مجموعه ای از کاربران یا کامپیوترها بکار می رود.

- از طریق Group Policy یا به اختصار GP می توانیم یک سری تنظیمات امنیتی و کاربردی را در سیستم انجام دهیم.
- در کامپیوترهای Local یا کامپیوترهایی که در یک Workgroup هستند، می توان یک GP را به همه ی کاربران اعمال کرد.
- بطور Default تمامی سیستم ها قبل از آنکه به عضویت Domain در آیند، از LGP یا Local Group Policy تبعیت می کنند. به محض عضویت در یک Domain، همگی از DGP یا Domain Group Policy تبعیت خواهند کرد.
- در یک شبکه ی Domain، اگر به هیچکدام از OU ها یا Site ها، GP اعمال نشود، از GP مربوط به Domain استفاده می کنند.
- می توانیم به ازای هریک Object و یا هریک OU در Domain، یک GP داشته باشیم، از اینرو Group Policy Object یا به اختصار GPO ، تعریف می کنیم.
- به هر Object، می توان تا 999 عدد GPO اعمال کرد.

LGP :

در حقیقت Group Policy هایی که خارج از Active Directory کار می کنند را Local GP می گویند، مثل GP های یک ویندوز Client. Local Policy های یک سیستم، در Directory زیر قابل مشاهده هستند:

C:\Windows\System32\GroupPolicy

ابتدا پنجره ی GP را با درج gpedit.msc در Run یا در Windows Search باز می کنیم.

همانطور که می بینیم، دو بخش اصلی دارد:

- **User Configuration :**
  شامل تنظیماتی است که بر روی User ها اعمال می شود بدون توجه به اینکه User با چه کامپیوتری Log On کرده است.

- **Computer Configuration :**
  شامل تنظیماتی است که بر روی Computer اعمال می شود، بدون توجه به اینکه چه User ای Log On کرده است.

Disable Local Users and Groups (lusrmgr.msc) :

User Configuration -> Administrative Templates -> Windows Components -> Microsoft Management Console -> Restricted/Permitted snap-ins

حال در کادر سمت راست، بر روی Local Users and Groups دابل کلیک کرده و آن را Disable می کنیم.

: User Password Policies

مسیر زیر را طی می کنیم:

Computer Configuration > Windows Setting > Security Setting > Account Policies > Password Policy

: Maximum Password age

- این پارامتر می تواند بین 1 تا 999 باشد.
- فرض کنید مدت زمان Maximum Password age روی 10 روز باشد.پس از 10 روز، اکانت بطور اتوماتیک قفل خواهد شد و پسورد دیگر کار نمی کند.
- اگر روی 0 باشد، یعنی پسورد اصلاً باطل نشود، که در اینصورت باید minimum pass age را عددی بین 0 تا 998 قرار دهیم.
- پس باید با حسابی که دسترسی Administrator دارد، وارد سیستم شد و یک پسورد جدید برای آن حساب کاربری تعیین کرد.
- معمولاً مقدار گزینه ی Maximum Password age را برای حساب Administrator یک سیستم، 999 قرار می دهیم.

: Lock the Account

وارد Account Lockout Policy می شویم.

- Account lockout threshold : تعداد دفعاتی که کاربر مجاز است Password اشتباه وارد کند.
- Account lockout duration : مشخص کننده ی مدت زمانی ست که حساب کاربری Lock خواهد ماند.
- Reset account lockout counter after : مشخص کننده ی مدت زمانی ست که لازم است تا شمارنده ی پسوردهای اشتباه، صفر شود.
- مقدار Reset account lockout counter after = < Account lockout duration می باشد.

: Auditing and Logging the Users

مسیر زیر را طی می کنیم:

Computer Configuration > Windows Setting > Security Setting > Local Policies > Audit Policy

توسط گزینه های این تب، می توان فعالیت های مختلف سیستم را در هر دو حالت موفقیت (Succes) و شکست (Failure) ثبت کرد.
می توانید دسترسی دیگران به فایل و پوشه ها را بطور مرتب چک کنید و فعالیت های آن ها را تحت نظر بگیرید.

مثلاً می خواهید ورود و خروج ها به حساب کاربری مورد نظرتان را بررسی کنید؛
پس گزینه ی Audit account logon events را باز کنید. Success و Failure را فعال کرده و Ok کنید.

برای مشاهده ی این ورود و خروج ها، در Run تایپ می کنیم eventvwr تا ابزار Windows Event Viewer باز شود.
در منو سمت چپ Windows Logs را باز کنید و از زیر منوی باز شده Security را انتخاب کنید تا لیست تمام ورود و خروج ها و زمان آنها را مشاهده کنید.

- Event ID مربوط به ورود موفق 4624 و ورود ناموفق 4625 می باشد، که می توانیم با ابزار Filter آنها را بهتر مشاهده کنیم.

مثلاً می خواهید بدانید چه User های ایجاد شده یا تغییر یافته یا حذف شده و یا تغییرنام داده اند،
با فعال سازی **Audit account management** می توانید این گزارشات را نیز ثبت کنید.

User Rights Assignment :

مسیر زیر را طی می کنیم:

Computer Configuration > Windows Setting > Security Setting > Local Policies > User Rights Assignment

گزینه های این تب، در مورد این هستند که چه کسانی می توانند آن گزینه ها (کارها) را انجام دهند.

به همین جهت، باید برای هریک از آنها، فرد یا افرادی را انتخاب کنیم.

چند گزینه ی مهم آن :

Access this computer from the network :

Change the System Time :

Change the Time Zone :

Take Ownership of files or other objects :

تعریف می کند که کدام User ها قادر به تغییر دادن مالکیت فایل ها برای خود هستند.

Security Options :

مسیر زیر را طی می کنیم:

Computer Configuration > Policies > Windows Setting > Security Setting > Local Policies > Security Options

Accounts: Rename Administrator Account :

یک نام متفاوت برای حساب Admin مشخص می کند تا تشخیص آن برای کاربران غیرمجاز ساده نباشد.

Interactive logon: do not require Ctrl + Alt + DEL :

فشردن دکمه های Ctrl+ Alt+ DEL برای ورود به سیستم ضروری نباشد.

در حقیقت با فعال بودن صفحه ای که نیاز به فشردن این دکمه ها برای ورود به سیستم دارد، نرم افزارهایی که از طریق ورود Boot قادر به شکستن پسورد یا پسوردهای حسابهای کاربری ورودی به سیستم هستند، عملاً بی کاربرد می شوند و قادر به شکستن پسوردها نخواهند بود.

Shut down: allow system to be shut down without having to logon :

در صفحه ی Log on بتوان Shut down کرد.

Run Access / Control Panel Access:

مسیر زیر را طی می کنیم:

User Configuration > Administrative Templates > Control Panel

- **Prohibit access to Control Panel را باز کرده و گزینه ی Enable را فعال می کنیم.**
- **Control Panel از دسترس کاربران معمولی خارج می شود.**
- **و همچنین امکان استفاده از دستورات مختلف Run هم غیرفعال می شود.**

کنترل منوهای General و Connection در Internet Option :

مسیر زیر را طی می کنیم:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel

و سپس می توان گزینه های زیر را فعال یا غیرفعال کرد:

Disable the Connection Page
Disable the General Page

Task Manager Access :

مسیر زیر را طی می کنیم:

User Configuration > Administrative Templates > System > Ctrl + Alt + Del Options

Remove Task Manager را باز کرده و Enable می کنیم.

Prevent to Installation the Softwares:

مسیر زیر را طی می کنیم:

Computer Configuration > Administrative Templates > Windows Components > Windows Installer

Turn off Windows Installer را باز کرده و آن را روی Enable قرار داده و دکمه ی کرکره ای پایین را روی Always تنظیم کرده و Ok.

USB, cmd, Registry, Softwares blocking :

مسیر زیر را طی می کنیم:

User Configuration > Administrative Templates > System > Removable Storage Access >

Removable Disks: Deny read access : جلوگیری از خواندن حافظه ی USB

Removable Disks: Deny write access : جلوگیری از انتقال فایل از کامپیوتر به حافظه ی USB

جلوگیری از اجرای : command prompt / Registry Editor / برخی برنامه ها / و یا اجرای فقط برخی از برنامه ها:

مسیر زیر را طی می کنیم:

User Configuration > Administrative Templates > System >

Don't run specified Windows applications : را باز کرده و پس از Enable کردن، با کلیک کردن روی Show، در لیست باز شده، اسم هریک از نرم افزارهایی که می خواهیم مانع Open شدن شان شویم را با پسوند .exe درج کرده و در پایان Ok.

Run only specified Windows applications : را باز کرده و پس از Enable کردن، با کلیک کردن روی Show، در لیست باز شده، اسم هریک از نرم افزارهایی که می خواهیم Open باقی بمانند را با پسوند .exe درج کرده و در پایان Ok.
در این حالت تقریباً تمام برنامه ها و ابزارها، به جز آنهایی که درج می کنیم، بلاک خواهند شد.

Prevent access to the command prompt : جلوگیری از اجرای پنجره های Command Prompt

Prevent access to registry editing tools : جلوگیری از اجرای پنجره های Registry Editor

: Prevent to IP Address Change

مسیر زیر را طی می کنیم:

User Configuration > Policies > Administrative Templates > Network > Network Connections

و گزینه ی **Prohibit TCP/IP advanced Configuration** را فعال می کنیم.

: Hidden the Hard drives

مسیر زیر را طی می کنیم:

User Configuration > Administrative Templates > Windows Components > File Explorer >

گزینه ی **Hide these specified drives in My Computer** را فعال کرده و سپس در همانجا نام درایو مورد نظر را انتخاب می کنیم.

: Desktop Settings

مسیر زیر را طی می کنیم:

User Configuration > Administrative Templates > Desktop > Desktop

DGP :

برای دسترسی به تنظیمات **Group Policy** برای شبکه های **Domain**، نیاز به ابزار **Group Policy Management** داریم که در گزینه ی **Tools** و سپس **Group Policy Management** قابل فراخوانی است.

محل ذخیره سازیِ **Policy** های شبکه ی **Domain** در **Directory** زیر قابل مشاهده هستند:

****نام کامپیوتر سرور**\SYSVOL**آدرس**RootDomain\Policies**

- در سمت چپ پنجره ی این ابزار، **Forest** ایجاد شده را می بینیم که در زیر گزینه های آن **Domain** ها و **Site** های آن، بطور جداگانه قرار دارند.
- اگر وارد **Domains** شویم، **Root Domain** را می بینیم که با ورود به آن، سیاست هایی که به شکل **default** برای تمام اعضای **Domain** تعریف شده اند را در قالب گزینه ی **default domain policy** می بینیم.
- همچنین تمام **OU** های تعریف شده برای **AD** را نیز می بینیم که برای ایجاد و نسبت دادن سیاست های مورد نیاز برای هریک از آنها، در همانجا اقدام می کنیم.

برای ایجاد تغییرات در **Default Policy** ها، باید روی default domain policy کلیک راست کرده و **Edit** را زد.

مهم ترین **Policy**، بعد از راه اندازی یک شبکه، تنظیمات **lock** یا قفل شدن **User** ها در **Computer** ها و قوانین **Password** هاست:

Computer Configuration > Policies > Windows Setting > Security Setting > Account Policies >

در اینجا می توان :

- زمان عمر یک پسورد، حداقل طول آن و اجباری یا اختیاری بودنِ پیچیدگیِ آن را تعیین کرد.
- زمان قفل شدن یک **Account**،
- تعداد دفعات مجاز برای اشتباه وارد کردن پسورد،
- و تعیین یک زمان برای **Reset** کردن تعداد دفعات اشتباه زده شده ی **Password** را مشخص کرد.

برای اینکه پس از تعیین یک **Policy**، بدون اینکه کامپیوتر **Restart** شود، فوری اجرا و عملی شود، می توان در **cmd** درج کرد:

gpupdate /force

از طریق **GUI** که به راحتی می توان تنظیمات **Group Policy** را پیدا کرد و تغییر داد، اما از طریق **PowerShell** ، مثلاً:

برای مشاهده ی تنظیمات **Password** مربوط به **Default Domain Policy**:

```
Get-ADDefaultDomainPasswordPolicy
```

یا

```
net accounts
```

برای ایجاد تغییر در تنظیمات **Default Domain Policy** ، مثلاً برای تغییر بیشترین زمان اعتبار **Password** ها:

```
Get-ADDefaultDomainPasswordPolicy | Set-ADDefaultDomainPasswordPolicy -MaxPasswordAge 100
```

: Policy Assignment

- در حقیقت برای اختصاص **Policy** در شبکه های **Domain** از **Group Policy Object** ها استفاده می شود.
- هم می توان برای **Computer** ها و هم می توان برای **User** ها، **GPO** تعریف کرد.
- و یا با اعمال یک **GPO** به یک **OU**، آن **GPO** به همه ی **User** ها و **Group** های درون آن نیز اعمال خواهد شد.

نکته: نمی توان به Container ها هیچگونه GPO ای اعمال کرد.

- یکی از راه های ساده برای تعریف **GPO** ها، از طریق کنسول **MMC** است.
- پس کنسول **MMC.exe** را باز کرده و از طریق **File** و **Add or Remove Snap ins**، گزینه ی **Group Policy Object Editor** را **Add** می کنیم.
- **Browse** را زده و تعیین می کنیم که می خواهیم برای یک **PC** و یا برای یک **User**، قوانین تعیین کنیم؛ و **Ok** و **finish**!

- اما راه فراگیر تر همان پنجره ی **Group Policy Management** است.

- همانطور که می دانیم سیستم یا سیستم هایی که **Domain Controller** شبکه هستند، قوی ترین و پر مشغله ترین سیستم در شبکه اند.پس باید یک سری **Policy** فقط برای خود آنها تعیین شود.
- در پنجره ی **Group Policy Management**، در سمت چپ، مسیر زیر را می رویم:

Root Domain نام **> Domain Controllers > Default Domain controllers Policy**

- کلیک راست کرده و **Edit** را می زنیم تا وارد تنظیمات **DC** یا **DC** ها شویم.

به دو روش می توان به یک **OU**، یک **Policy** اختصاص داد:

روش اول:

- روی **OU** موردنظر کلیک راست کرده و **"... Create a GPO in this domain, and"** را زده و یک نام برای آن درج کرده و یک **GPO** برای این **OU** ایجاد می شود.

روش دوم:

- پوشه ی **Group Policy Objects** را انتخاب کرده و در کادر سمت راست، کلیک راست کرده و **New** و ....
- سپس روی **OU** مورد نظر کلیک راست کرده و **Link an existing GPO** را می زنیم.

: Who can access the Domain

Computer Configuration > Windows Setting > Security Setting > Account Policies > Local Policies > User Rights Assignment > Allow Log on locally

افرادی که در اینجا تعریف می شوند، جدا از اینکه در بخش Group ها، این حق دسترسی را داشته باشند یا نه، می توانند وارد Domain شوند!

: File pushing

فرض کنید قصد داشته باشیم، یک فایل را در همه یا تعدادی از سیستم های شبکه قرار دهیم، و یا جایگزین یک فایل دیگر کنیم.
مثلاً ما می توانیم فایل hosts را [که در مسیر c:\windowns\System32\drivers\etc قرار دارد] **بطور دستی و هماهنگ شده، ویرایش و تنظیم کنیم، و سپس آن را در همه ی سیستم های عضو شبکه، جایگزین کنیم.**

نکته: اگر فایل منبع بر روی خود کامپیوترهای مقصد وجود داشته باشد، آدرس local را وارد می کنیم، مثلا برای فایل hosts که در همه ی سیستم ها ثابت است:

c:\windowns\System32\drivers\etc

درغیراینصورت، ابتدا باید فایل موردنظری که تنظیم کرده ایم را share کرده و آدرس shared شده ی آن را کپی می کنیم؛ که خواهد شد:
\\DC01\FileName.xxx

- **حال در کنسول Group policy Management، برای کامپیوترها یا User های موردنظر، یک OU تشکیل داده و برای آن OU یک GPO ایجاد می کنیم.**
- **وارد تنظیمات GPO شده و به مسیر زیر می رویم:**
  - برای اعمال به کاربر:

User Configuration > Preferences > Windows Settings > Files

  - برای اعمال به کامپیوتر:

Computer Configuration > Preferences > Windows Settings > Files

- **بر روی File، راست-کلیک کرده و New را می زنیم.**
- **در پنجره ی باز شده، در قسمت Action، نوع عملکرد این Policy را تعیین می کنیم.**

: Create بعد از اعمال Policy، با هر بار اجرای آن ، فایل مقصد که در قسمت Destination وارد شده است، چک می شود، در صورتی که فایل، در این مسیر وجود نداشته باشد، آن را کپی خواهد کرد. اما اگر این فایل از قبل وجود داشته باشد، هیچ اقدامی صورت نخواهد گرفت.

: Replace بعد از اعمال Policy، با هر بار اجرای آن، فایل مقصد قبلی در صورت وجود، حذف شده و فایل جدید جایگزین می شود.
در صورت عدم وجود فایل قبلی، فایل جدید تعیین شده، ساخته خواهد شد.
(درحقیقت این حالت، قابل توصیه است.)
نکته: در صورتی که فایلی حجیم را برای کپی انتخاب نماییم، انتخاب این حالت ممکن است موجب ایجاد ترافیک زیاد در شبکه گردد.

: Update بعد از اعمال Policy، با هر بار اجرای آن، تنها Attribute ای که در Policy تعیین کرده ایم، بر روی فایل مقصد چک و اعمال خواهد شد، اگر از قبل چنین فایلی وجود نداشته باشد، فایل جدید با این نام و تنظیمات در آنجا ایجاد خواهد شد.

: Delete بعد از اعمال Policy، با هر بار اجرای آن، فایل تعیین شده، در صورت وجود حذف خواهد شد.

- **در نوار Source Files، آدرس فایل موردنظر را وارد می کنیم.**

پس آدرس local آن، و یا آدرس UNC را وارد می کنیم.
نکته: اگر بخواهیم تمام فایلهای موجود در یک پوشه، در آدرس مقصد کپی شوند، کافیست در انتهای آدرسی که در قسمت Source File وارد کرده ایم، به جای نام فایل از علامت ستاره استفاده کنیم. مثال: \\servername\FolderName*
نکته: استفاده از ستاره، تنها برای کپی کردنِ فایل ها کاربرد دارد، و بر روی Folder ها اعمال نمی شود.

- **در نوار Destination File، آدرس فایل موردنظر را وارد می کنیم.**

در صورتی که در قسمت Source File، نام یک فایل را وارد کرده باشیم، در قسمت Destination Folder هم، نام فایل مقصد را به همراه مسیر آن وارد می کنیم.

نکته: درصورتی که در نوار Source File از علامت ستاره استفاده کرده باشیم، نوار Destination file به Destination Folder تبدیل می شود که باید مسیر پوشه ای را وارد کنیم که قرار است فایلها درون آن کپی شوند.

- **اگر این Policy را از مسیر User Configuration انجام می دهیم، حتما باید User account یا Computer account مورد نظر، حداقل دسترسی Read را برای دسترسی به فایل داشته باشد.**

- **اگر این Policy را از مسیر Computer Configuration انجام می دهیم، حتما باید Computer account موردنظر، مجوز دسترسی به فایل موردنظر را داشته باشد.**

Deploy a Software :

فرض کنید بخواهیم یک یا تعدادی نرم افزار را تحت شبکه (توسط GPO و بطورخودکار)، در اختیار User ها و Computer های دیگر قرار دهیم، که به این کار Deploy کردن گفته می شود.

به دو روش می توان از طریق GPO اقدام به نصب نرم افزار کرد:

- **Publish: نرم افزار موردنظر توسط خود کاربر قابل نصب خواهد بود. به این شکل که هرکاربر در پشت سیستم، باید به آدرس زیر برود:**

Published : Control Panel\Programs\Programs and Features

سپس در سمت چپ، گزینه ی Install a Program from the Network را می زنیم و در کادر وسطی، روی نرم افزار مورد نظر دابل کلیک می کنیم.

- **Assign: پس از Login کاربر بر روی سیستم، آن نرم افزار بصورت کامل و خودکار روی سیستم نصب خواهد شد و کاربر می تواند آن را اجرا کند.**
  - **البته توسط این تکنیک، نرم افزارهای سبک را deploy می کنیم، نه حجیم و سنگین.**
  - **تنها فایل های نصبی با پسوند msi را به سادگی پشتیبانی و deploy می کند.**
  - **برای نصب فایل های با پسوند exe. نمی توان به صورت مستقیم توسط GPS اقدام کرد و باید برای آنها zap file ایجاد نمود.**
  درحقیقت یک Zap file، یک فایل Text است که نحوه ی نصب یک فایل نصبی مثلاً با فرمت exe. را تعریف می کند.

معایب GPO Software Deploying :

- **اگر چند Package نرم افزاری را deploy کنیم، کنترلی بر اینکه کدامیک در ابتدا اجرا شود، نخواهیم داشت.**
- **هیچ گزارشی مبنی بر اینکه عملیات با موفقیت انجام شده است یا خیر، وجود ندارد.**

Publish deployment :

1. فایل نصب را آماده می کنیم.

- **در ابتدا در سیستم DC یک Folder با یک نام مناسب، در هرکجای سیستم ایجاد کرده و فایل msi را درون آن کپی می کنیم.**
- **حال باید آن را Share کنیم، که می توانیم آن را برای EveryOne اما تنها با قابلیت Read اشتراک گذاری کنیم.**

2. اگر بخواهیم هرکاربری که وارد یکی یا تعدادی از PC های شبکه شد، بتواند به این Software ، دسترسی داشته باشد:

- در GP Management ، وارد تنظیمات GPO ی مربوط به این کامپیوترها می شویم، به مسیر زیر:
Computer Configuration > Policies > Software Setting >
- ابتدا وارد Properties گزینه ی Software Installation شده و اطمینان می یابیم که در کادر وسط، گزینه ی ..Display the Deplo فعال باشد و OK!
- روی Software Installation کلیک راست کرده و به مسیر Sharing این DC رفته و فایل msi را انتخاب می کنیم.
\\DC-Name\FolderName
- حال باید انتخاب کنید که نرم افزار چگونه نصب شود: assigned یا publishd

- در GP Management ، وارد تنظیمات GPO ی مربوط به این User های موردنظر شده و به مسیر زیر می رویم:
User Configuration > Policies > Software Setting >
- ابتدا وارد Properties گزینه ی Software Installation شده و اطمینان می یابیم که در کادر وسط، گزینه ی ..Display the Deplo فعال باشد و OK!
- روی Software Installation کلیک راست کرده و New و Package را می زنیم و به مسیر Sharing فایل msi موردنظر رفته و آن را انتخاب می کنیم.
- حال باید انتخاب کنید که نرم افزار چگونه نصب شود، پس published را می زنیم، که کاربر برای نصب آن باید به مسیر زیر برود:
Published : Control Panel\Programs\Programs and Features
- اما اگر در همین کنسول Group policy management روی نرم افزار موردنظر کلیک راست کرده و Auto install را فعال کنیم؛ به محض اینکه کاربر سعی در باز کردن فایلی با پسوند مرتبط به این نرم افزار کند، این نرم افزار بطورخودکار شروع به نصب می کند. مثلاً نرم افزار Adobe Reader و فایل های PDF.
- برای حذف این نرم افزار، روی آن کلیک راست کرده و به All Tasks می رویم.
- برای نصب این نرم افزار پس از login کردن کاربر و یا برای تغییر حالت اختصاص این نرم افزار و یا گزینه های دیگر، وارد Properties آن و تب Deployment می شویم.
- برای بروزرسانی نرم افزار به نسخه ی جدید آن، ابتدا نسخه جدید را در شبکه share کرده و در تنظیمات GPO نسخه ی قدیمی، وارد Properties آن و تب upgrades شده و Add را زده و توسط Browse آن را پیدا و انتخاب می کنیم؛ و در پایین همان پنجره، توسط دو گزینه ی ...Uninstall the existing و ...Package can upgrade over می توان نحوه برخورد با نسخه ی قدیمی را تعیین کرد.

: Folder Redirection

در شبکه های Enterprise و Domain هر کاربر با نام کاربری تحت دامین خود به هر سیستمی که Login کند، یک پوشه حاویِ تنظیمات پروفایل و فایلهای کاربری او ایجاد خواهد شد و با توجه به اینکه این پوشه در همان کامپیوتر Local و در بخش Users ایجاد می شود با Login نمودن کاربر در سایر کامپیوترهای تحت دامین، یک پوشه ی دیگر حاوی تنظیمات پروفایل و فایلهای او در کامپیوتر دیگر ایجاد می شود و کاربر به پوشه یا پوشه های خودش موجود در کامپیوترهای دیگر، دسترسی نخواهد داشت.

با استفاده از Folder Redirection می توانید مسیر ذخیره سازی این پوشه یا پوشه ها را Redirect کنید.

دلیل استفاده از Folder redirection این است که کاربر با Login بر روی هر کلاینت در شبکه می تواند به پوشه ی پروفایل خود دسترسی داشته باشد و اطلاعات پروفایلش را بر روی سیستم جدید ببیند.البته این احتمال وجود دارد که شاهد کند بودن در زمان انتقال داده ها باشد و آن هم بدلیل عدم ذخیره سازی اطلاعات بر روی آن سیستم جدید است.

قابلیت Folder Redirection برای GPO ها، فقط برای User Configuration و در بخش Windows Setting است.

می بینیم که درون آن چندین پوشه ی از پیش تعیین شده وجود دارد.که باید برای هریک از این Folder ها، این قابلیت را فعال و تنظیم کرد، فقط کافی ست روی هریک کلیک راست و Properties را بزنیم.

: Mapped Drive with GPO

همانطور که می دانیم می توانیم به Share Directory مربوط به یک PC رفته و به پوشه ای که Share شده دسترسی داشت.

اما برای سرعت و سهولت در دسترسی، می توان در همان Share Directory روی آن کلیک راست کرده و map network drive را بزنیم.

اما در این روش، معایبی هم وجود دارد، مثلاً اگر IP تغییر کند و ...، باید دوباره از نو آن را متصل کرد!

اما از طریق GPO، تقریباً یکبار و برای همیشه، از آن پوشه، یک Map Drive تهیه کنیم.

- پس ابتدا به Share Directory آن فایل رفته و مسیر آن را کپی می کنیم.
- به AD DS رفته، یک OU جدید می سازیم و درون آن، با کلیک راست و New، گزینه ی Shared Folder را می زنیم.
- یک نام برای آن انتخاب کرده و برای Network Path، آدرسی که کپی کردیم را paste می کنیم و تمام!
- به GP Management می رویم.
- برای OU آن، یک GPO ایجاد کرده و وارد Edit می شویم.

روش اول: یک پوشه را در جایی درون تمام سیستم هایی که در این OU قرار دارند، Share می کند.

- به مسیر زیر می رویم:

Computer Configuration > Preferences > Windows Setting >

- بر روی Network Shares کلیک راست کرده و New و Network Share را می زنیم.
- Action را بر روی Create قرار می دهیم.
- روی دکمه ی ...در کنار Share name کلیک کرده و پوشه ی Share شده را در پایین دابل کلیک می کنیم.
- روی دکمه ی ...در کنار Folder Path کلیک کرده و مثلاً Desktop را انتخاب کرده و OK و OK.

روش دوم: یک پوشه را به عنوان یک درایو، در تمام سیستم هایی که در این OU قرار دارند، Share می کند.

- به مسیر زیر می رویم:

User Configuration > Preferences > Windows Setting >

- بر روی Drive Maps کلیک راست کرده و New و Mapped Drive را می زنیم.
- Action را بر روی Create قرار می دهیم.
- روی دکمه ی ...مربوط به نوار Location کلیک کرده و پوشه ی Share شده را در پایین دابل کلیک می کنیم.
- تیک Reconnect و Use را زده و یک حرف را برای نام این Drive انتخاب می کنیم.
- یکبار Restart می کنیم.

: Starter GPO

- می توان یک Group Policy پایه ایجاد کرد که GPO هایی که ساخته می شوند را نسبت به آن تعریف کرد. به این GPO پیش ساخته و پایه ای، Starter GPO گفته می شود.
- می توان موقع ایجاد یک GPO، یک Starter GPO ی ساخته شده را به آن ضمیمه کرد.

برای ایجاد Starter GPO :

- به پوشه ی Starter GPOs رفته و روی دکمه ی Create Starter GPOs Folder کلیک می کنیم و در کادر باز شده، کلیک راست کرده و New را می زنیم.
- پس از ایجاد، می توان با کلیک راست، آن را Edit کرد.
- می توان Starter GPO ها را Delete یا Copy و Cut و Paste کرد.

:GPO Backup and Restore

- Backup گیری از GPO ها، امری مهم و حیاتی است.
- پس به پوشه ی Group Policy Objects رفته و با کلیک راست بر روی GPO مورد نظر، Backup را می زنیم.
- یک آدرس برای ذخیره شدن، به آن می دهیم و تمام!

- برای بازگشت به حالت Backup یک GPO، در همان پوشه ی Group Policy Objects روی آن کلیک راست کرده و Restore from Backup را می زنیم.

:Import Backup

- فرض کنید که از یک GPO در Domain1، فایل Backup تهیه می کنیم.
- حال قصد داریم در Domain2، آن Backup را، بر روی یک GPO دیگر، overwrite یا Import کنیم.

- پس فایل Backup از GPO مربوط به DC1 را به DC2 منتقل می کنیم.
- حال درتنظیمات Group Policy در سیستم DC2 و در پوشه ی Group Policy Objects، روی GPO ی مورد نظر، کلیک راست کرده و Import Setting را می زنیم.البته در پایان اگر نام ها یا UNC Address ها، متفاوت باشند، گوشزد می کند که باید تغییر داده شوند!

- می توان Backup ها را بطور کلی هم مدیریت کرد، باید روی Group Policy Objects کلیک راست و Manage را زد.

: Delegation

همانطور که می توانیم کنترل یک Domain را در کنسول AD Users and Computers با کلیک راست بر روی آن، به یک User یا حتی گروهی از User ها delegate کنیم، همچنین می توانیم کنترل Group Policy Management را برای یک Domain، به یک User یا گروهی از User ها وکالت دهیم.

فقط کافی ست نام خود Domain را انتخاب کنیم و در کادر سمت راست، در آخرین تب یعنی Delegation، هر User دلخواه را اضافه کنیم.

: Restricted Group

Help Desk ها مسئول رسیدگی به درخواست های Client ها و رفع مشکلات سیستم های آنها هستند.
همچنین مسئول کارهایی مثل نصب یا حذف نرم افزارهای مختلف، نصب و به روزرسانی درایورها و غیره.
به همین دلیل این افراد باید به سیستم Client ها دسترسی کامل در حد Administrator داشته باشند.
اما این افراد نباید به main Domain و Server ها و Active Directory دسترسی Administrator داشته باشند.
و اینکه این افراد را عضو گروه Domain Admins کنیم، از نظر امنیتی، کاملاً اشتباه و خطرناک است.
در اینجا ابزار Restricted Group در کنسول Group Policy Management، بهترین راه حل است.

1. **یک Groups ایجاد کرده و User های موردنظری که جانشین Admin خواهند بود را عضو آن می کنیم.**
2. **یک OU برای کامپیوترهای Client موردنظر ایجاد کرده و یک GPO به آن اختصاص می دهیم.**
3. **وارد تنظیمات این GPO شده و به مسیر زیر می رویم:**

Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Restricted Groups

4. **روی آن کلیک راست کرده و گزینه ی Add Group را می زنیم.**
5. **برای Group، گروهی که برای User های جانشین ایجاد کردیم را وارد می کنیم و OK!**
6. **در پنجره ی بعدی با کادر بالایی کاری نداریم اما در کادر This group is a member of، توسط دکمه ی Add، گروه Administrators را اضافه می کنیم.**
7. **OK کرده و gpupdate /force و تمام!**

GPO Processing :

نکته: وقتی برای یک OU، دو عدد GPO تعریف کرده باشیم، اولویت با آن GPO ای است که در ردیف بالاتر قرار دارد، به عبارتی دارای Link Order کمتر باشد.

یک OU علاوه بر GPO هایی که به آن لینک شده اند، چه تحت تأثیر Policy های دیگر باشد، چه نباشد، قبل از همه ی Policy ها، تحت تأثیر Policy های مربوط به Default Domain Policy قرار دارد.
می توان گفت که OU مورد نظر، Policy هایی را از Default Domain Policy، به ارث برده است که Inheritence نام دارد.

- **اگر احیاناً میان GPO های درون یک OU با Default Domain Policy یک تداخل پیش بیاید یا سیستم مجبور به تصمیم گیری شود که کدام را در اولویت قرار دهد، همیشه اولویت با GPO ی با Link Order کمتر است.**

برای اینکه مطمئن شوید در میان Policy های موثر بر یک OU، کدام یک در اولویت تر است، می توان OU را انتخاب کرد و در کادر سمت راست، تب Group Policy Inheritence را باز کرد.

- **اگر واقعاً قصد داشته باشیم که رابطه ی Inheritence میان Default Domain Policy و OU مورد نظر، کاملاً حذف شود، می توانیم روی این OU کلیک راست کرده و Block Inheritence را بزنیم.**
- **اگر بخواهیم به هر قیمتی، Default Domain Policy بر همه ی OU ها موثر واقع شود، می توانیم روی آن کلیک راست کرده و Enforced را بزنیم. این قابلیت باعث می شود که حتی در صورت Block Inheritence بودن یک OU، باز هم روی آن اثر کند.**

- **به هرحال اگر در حالت عادی، برای Default Domain Policy گزینه ی Enforced را فعال کنیم، برای همه ی OU هایی که Block Inheritence نیستند، Default Domain Policy به اولین اولویت برای اعمال Policy به OU ها تغییر می کند.**

- **همانطور که می دانیم وقتی یک GPO را به یک OU متصل کنیم، این GPO بر روی همه ی User هایی که درون این OU قرار دارند، موثر واقع خواهد بود.**

- **برای اینکه تعیین کنیم این GPO ی متصل شده، به یک یا تعدادی از User های این OU بی تأثیر باشد، در پوشه ی Group Policy Objects، این GPO را انتخاب کرده و در کادر سمت راست و تب Scope و در پایین خواهید دید که در بخش Security Filtering، گزینه ی Authenticated Users انتخاب شده است.**
  یعنی این GPO بر روی همه ی User هایی که Authenticated شده باشند، اعمال خواهد شد.
- **پس می توانیم این گروه را Remove کرده و User های مورد نظر را وارد کرد و یا اینکه User های مورد نظر را در یک Group عضو کرد و این Group را وارد کرد.**

- **فرض کنید می خواهیم تعیین کنیم که یک GPO فقط به User هایی که با Windows 10 بالا می آیند، موثر واقع شود.**
- **پس وارد پوشه ی WMI Filters (Windows Management Interface) می شویم و در کادر آن، کلیک راست کرده و New را می زنیم؛ یک Name برای آن تعیین کرده و در کادر Queries یک دستور برای شناسایی ویندوز User وارد شده درج می کنیم.**
- **سپس دوباره GPO مورد نظر را انتخاب کرده و در تب Scope، در قسمت WMI Filtering ، گزینه ی Query درج شده را می زنیم.**

Loopback Processing :

همانطور که می دانیم هر **Policy** که ایجاد می کنیم، دارای دو بخش تنظیمات **User** و تنظیمات **Computer** است.
فرض کنید در یک شبکه دو **OU** با نام های **Server-OU** و **User-OU** وجود دارند که به ترتیب **Server** ها و **User** های شبکه را درون آنها قرار داده ایم و در کنسول **Group Policy** ها، به هریک از این **OU** ها، **GPO** های متفاوتی را اختصاص داده ایم.

حال اگر **UserA** بر روی یکی از **Server** ها **Log in** کند، **Policy** هایی که به آن اعمال می شوند به ترتیب زیر خواهند بود:

- **Computer Configuration** مربوط به **GPO** ی **Server-OU**.
- **User Configuration** مربوط به **GPO** ی **User-OU**.

حال یک **Option** وجود دارد به نام **Loopback** با دو حالت متفاوت:

➢ **Replace :**
اگر **UserA** بر روی یکی از **Server** ها، **Log in** کند، **Policy** هایی که به آن اعمال می شوند، بصورت زیر هستند:
- **Computer Configuration** مربوط به **GPO** ی **Server-OU**.
- **User Configuration** مربوط به **GPO** ی **Server-OU**.

➢ **Merge :**
اگر **UserA** بر روی یکی از **Server** ها، **Log in** کند، **Policy** هایی که به آن اعمال می شوند، بصورت زیر هستند:
- **Computer Configuration** مربوط به **GPO** ی **Server-OU**.
- **User Configuration** مربوط به **GPO** ی **Server-OU**.
- **User Configuration** مربوط به **GPO** ی **User-OU**.

در صورت بروز تداخل، اولویت اجرای **Policy** ها مربوط به **GPO** ی **Server-OU** خواهد بود.

برای دسترسی و تغییر قابلیت **Loopback Processing**، روی **GPO** کلیک راست کرده و **Edit** را می زنیم و به مسیر زیر می رویم:
Computer Configuration > Policies > Administrative Templates > System > Group Policy >
Configure User Group Policy Loopback Processing Mode
پس ابتدا آن را **Enable** کرده و سپس یکی از گزینه های **Mode** را انتخاب می کنیم.

نکته:
در همین پوشه ی **Group Policy** گزینه ای وجود دارد که می توان با آن تعیین کرد که اگر سرعت (**Band Width**) یک سیستم یا شبکه کمتر از یک مقدار خاصی بود، یک سری پردازش ها قطع شوند:
Configure Group Policy Slow Link Detection
پس از **Enable** کردنِ آن، باید تعیین کنیم که اگر سرعت از چه حدی پایین تر برود، برخی **Proccess** های کم اهمیت تر قطع شوند یا وصل نشوند.

Script Logon/Logoff :

گاهی لازم است که با ورود به سیستم یا در هنگام خروج از سیستم، یک سری عملیات را بطور خودکار برای یک **User** یا برای یک **PC** اجرا کنیم، که این عملیات توسط یک سری دستور **PowerShell** یا **CommandPrompt** اعمال می شوند.
برای وارد کردن این دستورات، وارد **GPO** ی مورد نظر شده و بسته به نیاز، وارد **Computer/User Configuration** شده و در مسیر زیر:
Policies > Windows Setting > Scripts (Startup/Shutdown)
حال در یکی از دو گزینه ی روبرو تنظیمات را وارد می کنیم.

Security Template :

همانطور که می دانیم برای **Group Policy** ها، بخش **Seurity Setting** برای **Computer Configuration** خیلی مهم و اساسی است.
به همین جهت می توان یک **Template** ایجاد کرد تا در مواقع لازم، آن را **Import** کرده و مابقی تغییرات را روی آن اعمال کنیم.

برای ایجاد یک **Security Template** می توان در کنسول **MMC** در کادر سمت چپ پنجره ی **Add or Remove Snap ins** گزینه ی **Security Templates** را **Add** کرده و آن را انتخاب کرده و در کادر وسط، کلیک راست و **New** را زده و یک نام تعیین کرده و **OK** می کنیم.
وارد زیر گزینه های آن شده و تغییرات مورد نظر را اعمال کرده و در پایان با کلیک راست بر روی خود **Template** ای که ایجاد کرده ایم، **Save as** را زده و ذخیره اش می کنیم.
برای اعمال کردن آن به یک **GPO**، کافی ست وارد تنظیمات آن **GPO** شده و در بخش **Computer Configuration** و روی گزینه ی **Security Setting** کلیک راست و **Import** را بزنیم.

Group Policy Preferences :

ما می توانیم برای یک سری از تغییرات پیشفرض دلخواه و موجودیت های دلخواه را برای **User** ها یا **PC** هایمان ایجاد کنیم.

- مثل ایجاد یک **Folder** برای یک یا تعدادی **User** و اختصاص آن فقط به آنها در یک آدرس خاص و ....
- اشتراک گذاری پرینتر
- اشتراک گذاری یک پوشه یا **Drive** به عنوان یک **Map Drive**
- تغییر نام حساب های **Administrator** کامپیوترها
- ایجاد یک حساب دلخواه برای هر کامپیوتر (Local Users and Groups)

و تمام این تنظیمات را می توانیم با یک سری پیش شرطها نیز تعریف کنیم.
مثلاً برای همه ی **User** های یک **OU** تعیین کنیم که بتوانند از **Printer** استفاده کنند.

اما حالا می توانیم تعیین کنیم که از این **User** ها، فقط آنهایی که **RAM** بالای مثلاً **2024** و ویندوز بالاتر از **10** و ... دارند، بتوانند.
پس از تعیین تنظیمات گزینه ی مورد نظر در **Windows Preferences** در تب **General**، سپس به تب **Common** رفته و گزینه ی **Item-Level Targeting** را فعال کرده و دکمه ی **Targeting** را زده و در پنجره ی جدید، **New Item** را زده و به سادگی هریک از پیش شرط های مورد نظر برای هریک از گزینه ها را می توانیم تعیین کنیم.

Password Object :

تمام تنظیماتی که در Default Domain Policy اعمال می شود، بر روی همه ی User های شبکه اعمال می شوند.

ما می توانیم یک GPO ایجاد کرده و تنظیمات مورد نیاز را در آن اعمال کنیم و سپس GPO را به یک OU لینک کنیم، اما در مورد Account Policy ها بی فایده است.

کاربران و کامپیوترهای عضو آن OU در بحث Account Policy کماکان تابع Default Domain Policy خواهند بود.

فرض کنید که می خواهیم تنظیمات Password را برای فقط یکی یا تعدادی از User های خاص تعریف کنیم.

- پس وارد کنسول Active Directory Administrative Center می شویم.
- در کادر سمت چپ، گزینه ی «نام Domain» را انتخاب می کنیم.
- در بالا، سمت راست، وارد Manage شده و Add Navigation Nodes را می زنیم.
- در پنجره ی جدید، در کادر وسطی، System را انتخاب می کنیم و در کادر سمت راستِ آن، Password Setting Container را پیدا کرده و روی آن دابل کلیک کرده و پنجره ی آن را با OK می بندیم.
- حال می بینیم که در سمت چپ، یک پوشه ی جدید برای شبکه ی Domain مان با پسوند Password Setting ایجاد شده است، آن را انتخاب می کنیم.
- حال باید یک Password Object ایجاد کنیم، پس در کادر Task در سمت راست، New و Password Setting را می زنیم.
- ابتدا یک Name برای آن تعیین می کنیم.
- در نوار Precedence باید اولویت این Password Object را تعیین کنیم که عدد یک، بالاترین اولویت را دارد.
- سپس تنظیمات مورد نیاز برای Password را اعمال می کنیم.
- در پایان باید تعیین کنیم که این Password Object بر روی کدام User ها اعمال شود، پس در پایین سمت راست، Add می کنیم.

Reset the GPO :

اولاً برای اینکه Group Policy Management را بطور کلی و خودکار بررسی کنید که اگر اشکالی یا قطعی ای وجود داشته یا دارد، متوجه شوید، کافی ست، در کنسول GP Management ، گزینه ی خود Domain را انتخاب کرده و در کادر سمت راست و پایین، دکمه ی Detect Now را بزنید.

برای ریست کردن Domain GPO، در CMD درج می کنیم:

dcgpofix /target:Domain

برای ریست کردن Default DC GPO، در CMD درج می کنیم:

dcgpofix /target:DC

برای ریست کردن هم Domain و هم Default DC GPOs ، در CMD درج می کنیم:

dcgpofix /target:both

Reset the Group Policy :

نکته: تنها زمانی که به اشتباه تمام دسترسی ها را حتی برای خود حساب Administrator قفل کرده ایم، نیاز به این کار داریم.

ابتدا Restart کرده و از طریق یک USB یا CD ویندوز، وارد مراحل نصب می شویم و در اولین مرحله ی تنظیمات نصب، با فشردن دکمه های shift + F10 پنجره ی CMD را باز می کنیم.
ابتدا لازم است که مطمئن باشیم که ویندوز بر روی کدام Partition نصب بوده است، پس تایپ می کنیم: diskpart
سپس تایپ می کنیم: list volume
وقتی از نام درایو ویندوز مطمئن شدیم، با درج Exit و فشردن Enter به محیط cmd باز می گردیم و کد زیر را تایپ و اینتر می کنیم:
RD /S /Q "D:\Windows\System32\GroupPolicy"
سپس کد زیر را نیز درج و اینتر می کنیم و خارج شده و به حالت معمولی وارد سیستم می شویم:
RD /S /Q "D:\Windows\System32\GroupPolicyUsers"

Gpresult :

در شبکه های بزرگ که GPO های زیادی را تنظیم و در شبکه اعمال می کنیم، گاهی که مشکلاتی به وجود می آیند، در اثر اختلال GPO ها و یا عدم اعمال یکی یا تعدادی از GPO ها خواهند بود.

- برای اینکه وضعیت اعمال همه ی GPO هایی که بر روی یک سیستم اعمال شده اند را مشاهده و بررسی کنیم، کافی ست بر روی آن سیستم، وارد cmd شده و دستور زیر را وارد کنیم:

gpresult /r

پس اطلاعات کلی مربوط به GPO های اعمال شده به سیستم، هم مربوط به User settings و هم مربوط به Computer settings را لیست می کند.

- فرض کنید بخواهیم که همین نتیجه را، تنها مربوط به User و یا فقط مربوط به Computer settings دریافت کنیم؛ پس:

gpresult /r /scope:computer

gpresult /r /scope:user

- اگر بخواهیم که اطلاعات خیلی جزیی تر از GPO های اعمال شده به سیستم، را دریافت کنیم، پس نیاز است که نتیجه را به شکل یک فایل HTML دریافت کنیم. پس از دستور زیر استفاده می کنیم:

gpresult /h Test.html

پس فایل Test.html در مسیر c:\windows\system32 ذخیره می شود؛ اما جهت تغییرمسیر ذخیره ی این فایل:

gpresult /h d:\PoosheyeDelkhah\Test.html

- درحقیقت، تمام نتایجی که تا اینجا دریافت می کنیم، مربوط به Computer و user account جاری (login کرده) می باشد. اما اگر بخواهیم که تنظیمات GPO اعمال شده بر روی User account دیگری تحت این سیستم را دریافت کنیم:

gpresult /h d:\PoosheyeDelkhah\Test.html /User DomainName\Username

Snapshot :

در واقع این قابلیت، یک Backup لحظه ای یا یک image از Active Directory است.
بدون این قابلیت، ناچاریم که از درایو C یک system state backup بگیریم که زمان زیادی می برد و حجم بالایی هم خواهد داشت.
اما Snapshot حجم کمی دارد.
Snapshot ها در درایوی که دیتابیس Active Directory در آن قرار دارد، ذخیره می شوند، ولی قابل مشاهده نیستند.
برای ایجاد Snapshot هم از ابزار ntdsutil و ترتیب از دستورات زیر استفاده می کنیم:

1. Ntdsutil

2. Activate instance ntds

3. Snapshot

برای دیدن قابلیت های دستور Snapshot :

4. ?

5. Create

پس از اتمام Snapshop، سعی می کنیم یکبار یک لیست از آن فراخوانی کنیم:

6. List all

برای فراخوانی یک Snapshot:

7. mount شماره ی اسنپشات

حال این Snapshot در مسیر و با نام مشخص شده، ذخیره شده است.پس با درج Quit، کاملاً از NTDSutil خارج می شویم.

برای اینکه آن را اجرا کنیم، ابتدا باید آدرس آن را کپی کرده و بصورت زیر در CMD وارد کنیم (شماره پورت را می توان 50000 وارد کرد):

8. DSAmain -Dbpath C:\$SNAP_202008181350_VOLUMEC$\Windows\NTDS\ntds.dit -ldapport 40000

حال برای جایگزین کردن این Snapshot در درون Active Directory، وارد Users and Computers می شویم، و روی اولین گزینه ی سمت چپ، یعنی Active Directory Users and Computers کلیک راست کرده و Change Domain Controllers را می زنیم و در پنجره ی باز شده، در کادر پایین، روی گزینه ی Type a directory Server Name زده و نام کامپیوتری که Snapshot را روی آن mount کرده ایم، همراه با پورت ldap ای که فراخوانی کردیم، به شکل زیر وارد می کنیم:

PC1:40000

حال بطور خودکار شروع به جستجوی AD Database روی پورت 4000 می کند و بالاخره Online می شود.

برای Unmount کردن این Snapshot، دوباره cmd را باز کرده و به ترتیب درج می کنیم:

9. Ntdsuilt
10. Activate instance ntds
11. Snapshot
12. List all
13. Unmount شماره ی اسنپ شات
14. Quit
15. Quit

Services :

تمام ارتباطات لازم و اساسی ای که در سیستم عامل ویندوز باید برقرار باشند تا از ساده ترین خدمات سیستم مثل گوش دادن به موسیقی و دیدن عکس و فیلم تا خدمات پیچیده تری مثل ارتباطات پیچیده ی چند کامپیوتر یا چند شبکه، توسط سرویس هایی که درون سیستم عامل مدام در حال اجرا هستند، پیگیری و انجام می شوند.

مهمترین تفاوتی که بین یک **Service** و یک برنامه ی کاربردی وجود دارد این است که شما می توانید محیط یک برنامه را مشاهده کنید، اما نمی توانید محیط سرویس را مشاهده کنید! در واقع تمامی سرویس ها در پیش زمینه یا **Background** سیستم عامل مشغول به فعالیت هستند و شما متوجه اجرا شدن آنها نمی شوید.

در واقع سرویس ها **User Interface** ندارند!

سرویس ها برای ارائه ی خدمات پایه ایِ سیستم عامل، طراحی و تولید می شوند.

وقتی وارد یک وبسایت می شویم،

وقتی که به یک **File Server** متصل می شوید و یا سیستم خودتان یک **File Server** می شود،

وقتی که یک از یک **Printer** استفاده می کنید و یا حتی وقتی یک خطا مشاهده می کنید،

در واقع هریک از این اتفاقات، در یک سرویس در حال انجام شدن است.

سرویس های سیستم عامل ویندوز، برگرفته از ماهیت **Daemon** در سیستم عامل **Unix** هستند.

همه سرویس هایی که بر روی ویندوز نصب می شوند، مربوط به خود شرکت مایکروسافت نیستند!

برخی از **Application** ها و **Driver** ها برای خودشان سرویس هایی دارند که بصورت جداگانه بر روی سیستم عامل نصب می شوند.

مثلاً زمانیکه یک **AntiVirus** نصب می کنید، بصورت خودکار این نرم افزار سرویس خودش را بر روی سیستم عامل نصب می کند.

یکی از مهمترین مزایای سرویس ها این است که می توانند قبل از **boot** شدن کامل سیستم عامل و یا قبل از ورود به سیستم و اجرای برنامه ها، اجرا شوند.

یکی از ویژگی های مهم آنها این است که می توانند به راحتی با هسته اصلی سیستم عامل شما ارتباط برقرار کنند و با هر چیزی که در این هسته وجود دارد می توانند یکپارچه شوند.این باعث می شود که سرویس ها بتوانند سطح **Security** خوبی را در اختیار برنامه ها قرار دهند.

دانستن اینکه هر کدام از سرویس ها چه کاری انجام می دهند و چه نیازی را برطرف می کنند بسیار مهم است و می تواند در بسیاری از موارد باعث بالا رفتن کارایی سیستم عامل شود.و یا مثلاً وقتی یک سرویس در سیستم عامل شما کاری انجام نمی دهد و نیازی به استفاده از آن نیست، می توان آن را غیرفعال کرد که باعث افزایش سرعت سیستم می شود.

مثلاً سرویسی در سیستم عامل ویندوز وجود دارد که برای به اشتراک گذاری اینترنت است: **Internet Connection Sharing**

می توان برای اجرا کردن سرویس ها، اولویت بندی تعیین کرد، تا سرویس های حیاتی زودتر روشن شوند. به این صورت که یک سرویس کم اهمیت تر را در حالت **Delayed Startup** قرار می دهیم تا بعد از اجرا شدنِ همه ی سرویس های مهم تر، **Run** شود.

- سرویس ها معمولا در هنگام **Boot** سیستم عامل، اجرا می شوند.
- می توان سرویس ها را براحتی **Stop** و **start** کرد.
- سرویس ها در **Session** هایی مجزا از **Windows Session** اجرا می شوند، که معمولا **Session** صفر هستند.
- **Session** صفر به این معناست که همه ی کاربران بصورت همزمان قادر به استفاده از سرویس ها هستند.
- سرویس ها را می توانید چرخدنده های ساعت در نظر بگیرید! صحت کارکرد و بازده ای ساعت وابسته به آنهاست، ولی شما آنها را نمی بینید.

Kerberos :

در حقیقت ویندوز Server با استفاده از دو پروتکل زیر، عملیات امنیتیِ میان User ها ، PC ها و Service ها را انجام می دهد:

- Kerberos : که آخرین نسخه ی آن 5 است.
- NTLM (NT Lan Manager): که پروتکل قدیمی Microsoft است و امروزه در عرض چند ساعت، قابل هک شدن است!

امروزه پروتکل Authentication پیش‌فرض در ویندوزهای ماکروسافت، Kerberos می باشد.
اما اگر کامپیوتری در شبکه، از Kerberos V5 پشتیبانی نکند، به جای آن از NTLM استفاده خواهد کرد.

پس وظیفه ی پروتکل Kerberos ارائه ی خدمات AAA در محیط Domain است.

- Authentication
- Authorization
- Accounting

یک پروتکل تحت شبکه است که در سطحی گسترده برای حل مشکل Authentication استفاده می‌شود.
کربروس از رمزنگاری کلید متقارن (Symmetric key) و مرکز توزیع کلید KDC یا Key Distribution Center استفاده می‌کند.
که این KDC درون هریک از DC هایی که سرویس AD Users and Computers را دارند، قرار دارد.

Kerberos برای Authentication، به مجوز سومی که مورد اعتماد باشد، نیاز دارد، به همین جهت به آن thrid-party Service گفته می شود.

Kerberos همچنین اینترنت را به محیطی امن‌تر تبدیل کرد و این امکان را برای کاربران فراهم کرد تا بدون نگرانی، در دفتر کار خود با اینترنت کار کنند.

وقتی که کاربر تلاش می کند به یک کامپیوتر تحت دامین Log on کند، درخواست Authentication اش، برای DC ارسال می شود.
هر DC در شبکه،)است.
KDC پس از تایید هویت کاربر، به او یک TGT (Ticket-Granting Ticket) می دهد.
البته به شرطی که فاصله ی زمانی بین ارسال درخواست کاربر و رمزگشایی درخواست توسط Kerberos ، از 5 دقیقه تجاوز نکند که البته این مقدار زمانی هم قابل تغییر است.

Kerberos از دو نوع سیستم نامگذاری عناصر شبکه استفاده می کند:

- UPN (User Principal Name): که برای نامگذاری User ها و Computer ها استفاده می شود.
  مثلاً آدرس UPN مربوط به کاربری با نام Ali در شبکه ی Payamavar.local می شود: ali@payamavar.local
  این آدرس در تمام Forest یکتاست.

- SPN (Service Principal Name):
  به هر اتصال و استفاده از یک Service، یک Instance گفته می شود.
  برای نامگذاری هریک از Instance ها، از SPN استفاده می شود.
  در حقیقت، می توان چندین Instance از یک Service داشت، اما با SPN های متفاوت

- **Principal** : به Service ها، System ها، User ها و کلیه عناصری که نیاز به شناساندن خود به Kerberos دارند، گفته می شود.

در حقیقت هر Application برای اجرا شدن و انجام کارهای خود، احتیاج به استفاده از Service هایی دارد.
Kerberos بررسی می کند که آیا یک User یا Application، مجاز به استفاده از سرویسی که تقاضای اجرای آنرا دارد هست یا نه.
مثلاً بیشتر برنامه های حسابداری مبتنی بر SQL Server، با سرویس های ریز و درشت SQL سر و کار دارند.

زمانی که کاربر نیاز دارد که از یک سرویس در Domain خودش استفاده کند:

- سیستم کاربر باید یک Service Ticket معتبر جهت ارائه به کامپیوتری که سرویس مورد نظرش روی آن در حال اجراست، داشته باشد.
  - Service Ticket هم توسط KDC در DC فراهم می شود.
- پس کاربر درخواست Service Ticket خود را به DC می فرستد.
- از آنجا که کاربر قبلا Authenticated شده است، دارای TGT است و TGT خود را همراه با درخواستش ارسال می کند تا KDC بدون آنکه دوباره عمل Authentication را انجام دهد، Service Ticket را برای او صادر کند.
- KDC یک نمونه از Service Ticket را برای سروری که سرویس مورد نظرِ کاربر روی آن قرار دارد نیز می فرستد.
- و بالاخره کاربر می تواند با استفاده از Service Ticket به سرویس مطلوب متصل شود.
- Server مقصد قادر است تا Service Ticket را بررسی و کنترل کند که آیا کاربر Authenticated شده است یا نه.
- این کنترل و بررسی با استفاده از Private Key انجام می شود.

Ticket : نوعی Certificate یا تأییدیه است که هنگام ورود کاربر به قلمرو Kerberos ، به کاربر داده می شود که به معنای مجاز بودن کاربر برای دسترسی به منابع شبکه است.

نکته: Kerberos از قابلیت SSO (single sign-on) استفاده می کند، یعنی کاربرها فقط برای اولین بار که وارد می شوند، Authenticate شده و Ticket را دریافت می کند و در دفعات بعدی، نیاز به تایید هویت مجدد نیست.

Ticket Distribution Center : بخشی از Server است که اگر Authentication مثبت بود، Ticket را به کاربر می دهد.

Service Delegation :

برای اینکه یک **PC** بتواند از یک یا چند **Service** در یک کامپیوتر دیگر استفاده کند، باید به این **PC** مجوز دسترسی به آن **Service** را اعطا یا **delegate** کنیم.
برای وکالت دادن این مجوز دسترسی به **Service** مورد نظر، برای این **PC** :
در **Active Directory Users and Computers** وارد **Properties** مربوط به این **PC** شده و در تب **Delegation** سه گزینه وجود دارد:

- **... Don't trust this Computer for** : یعنی اصلاً به این **DC** جهت اعطای مجوز سرویس، مجوز نده!
- **.. Trust this Computer for** : یعنی جهت اعطای هرگونه سرویسی، اما فقط تحت پروتکل **Kerberos** مجوز بده!
اگر این نوع اعطای دسترسی را انتخاب کنیم، به این نوع دسترسی **Unconstrained Delegation** گفته می شود.
- **.. Trust this Computer for delegation to specified** : یعنی فقط جهت دسترسی به **Service** های مشخص شده، مجوز بده.
اگر این نوع اعطای دسترسی را انتخاب کنیم، به این نوع دسترسی **Constrained Delegation** گفته می شود.

در نتیجه گزینه ی سوم را زده و یکی از گزینه های مربوط به نوع پروتکل را انتخاب و در پایین همین تب، از طریق دکمه **Add**، کامپیوتر مقصد که سرویس مورد نظر را دارد انتخاب می کنیم، سپس پنجره ی **Add Services** باز می شود و سرویس مورد نظر را نیز انتخاب می کنیم و تمام!

Service Account :

همانطور که User ها و Computer ها دارای یک Account می باشند، سرویس ها نیز دارای یک Account هستند و این حساب کاربری که به Service Account موسوم است، اهمیت بسیار زیادی دارد.
Application ها از آن برای دسترسی به Service های موجود در سیستم عامل استفاده می کنند.

اگر در کنسول Services، وارد Properties یک Service شوید، در تب Log On خواهید دید که می توان نوع Service Account برای دسترسی به این سرویس را معین کرد. انواع معمول Service Account ها به ترتیب زیر هستند:

1. Local system : که Type آن 0 است و بطور built-in است.

- بالاترین سطح دسترسی و مدیریت و اولویت را دارد و در حقیقت از طریق خود حساب کاربریِ فعلی موجود روی سیستم، به این Service متصل می شود.

2. Batch : که Type آن 4 است.

- برای کارهای برنامه ریزی شده (Scheduled Tasks) می باشد.
- مثل زمانی که شما نرم افزار Backup داخل ویندوز را برای اجرا در زمان های معین و با حساب کاربری معینی برنامه ریزی می کنید.
- این نوع Logon اغلب برای Batch Server ها به کار می رود که در آنها، پردازش ها می توانند با حساب کاربری یک کاربر و بدون دخالت مستقیم آن کاربر، اجرا شوند.
- همچنین برای سرور هایی با کارایی بالا، که تعداد زیادی احراز هویت ها را پردازش می کنند، مثل Mail Server ها و Web Server ها، این نوع Logon انجام می شود.
- کاربران خرابکار نیز از این Logon و از طریق Scheduled Tasks برای حدس زدن گذرواژه ی حساب کاربری، مثل حساب کاربری Administrator استفاده می کنند!

3. Local Service : که Type آن 5 است و بطور built-in است.

- کمترین دسترسی به منابعِ سیستم عامل را دارد.
- درست مانند Scheduled Task ها تحت یک حساب کاربری تعریف شده، اجرا می شوند.این نوع Logon، برای سرویس ها و حساب های کاربری ای که برای شروع سرویس ها به کار می روند (Service Accounts)، می باشند.

طبق توضیحات بالا، بهترین نوع، Local System است. اما دو مشکل وجود دارد، یکی اینکه، دسترسیِ زیادیِ آن، مشکلات امنیتی خواهد داشت، و همچنین خیلی از سرویس ها، این نوع Service Account را پشتیبانی نمی کنند.
پس مجبور خواهیم بود که از User های معمولی که در AD Users and Computers ایجاد می شوند، به عنوان Service Account استفاده کنیم. به این معنا که تعیین می کنیم Application ها، با این User به این Service موجود در Server متصل شوند.

فرض کنید بخواهیم یک نرم افزار اجرایی مثل Notepad را توسط یک Service و با دسترسی Local برای یک User اجرا کنیم:

- ابتدا در Active Directory یک User برای آن تعریف می کنیم: مثلاً User ای به نام NotServ
- سپس یک Service برای آن ایجاد کنیم:
- PowerShell را با دسترسی Admin باز کرده و درج می کنیم:

New-Service یک نام برای سرویس -BinaryPathName مسیر ذخیره سازی فایل اجرایی نرم افزار مورد نظر

New-Service abc -BinaryPathName C:\Windows\system32\notepad.exe

- پنجره ی Services را باز کرده و سرویس abc را پیدا کرده و وارد Properties آن می شویم و در تب Log On در قسمت This Account، مشخصات حساب کاربری NotServ را وارد می کنیم و تمام.

نکته: البته می توان به جای ایجاد یک User و وارد کردن مشخصات آن برای تب Log On، یک User مجازی را برای آن فراخوانی کرد. به این صورت که برای نام this Account درج می کنیم:

NT SERVICE\نام سرویس

NT SERVICE\abc

و جای Password را کاملاً خالی می کنیم، که پس از OK کردن، خود سیستم یک پسورد اختصاص می دهد.

حال مشکلی که User های معمولی دارند، این است که تمام این User ها، باید بعد از یک مدت معین، تغییر Password دهند! فرض کنید که ما دسترسی به تعداد زیادی Service را از طریق این User ها تعریف کرده باشیم؛ به محض تغییر پسورد آنها، مجبوریم این پسورد جدید را در تمام تنظیمات Service ها نیز اعمال کنیم، که به قطع، کاری زمانگیر و طاقتفرساست!

به همین دلیل دو نوع Service Account وجود دارند که از Windows 2008 به بعد پدید آمدند و کاربرد حرفه ای تری دارند و دو قابلیت مهم را به Service مورد نظر می دهند:

- خودکارسازی عملیات مربوط به Password ها
- مدیریت نامِ سرویس ها (Service Principal Name)

1. MSA (Managed Service Account) :

البته آنها را بنام sMSA نیز می شناسند، یعنی MSA استاندارد.

این Service Account یک پسورد Random و شامل 240 کاراکتر برای سرویس مورد نظر ایجاد می کند و به صورت پیش فرض و خودکار، هر 30 روز یکبار آنرا تغییر می دهد.

2. gMSA (group MSA) :

مشکلی که MSA ها دارند، این است که هر MSA را فقط به یک PC می توان اختصاص داد و نه بیشتر!

پس اگر بخواهیم برای تعداد زیادی PC ، تک به تک MSA ایجاد کنیم، باز هم عملیاتی وقتگیر و طاقتفرسا خواهد بود.

پس gMSA ها پدید آمدند و می توان به تعداد زیادی PC یک gMSA را اختصاص داد.

از جمله سرویس ها یا **Application** هایی که نیازمند این **Service Account** های با مدیریت خودکار رمز عبور هستند:

- **SQL Server**
- **Exchange Server**
- **IIS**

در کنسول **AD Users and Computers** و در **Container** ای به نام **Managed Service Accounts** می توان سرویس اکانت های **MSA** را مشاهده کرد که در ابتدا خالی است.

: Create a sMSA

- در حقیقت وقتی یک MSA را می سازیم، فقط ساخته شده است!
- یعنی MSA هنوز به هیچ سیستمی متصل نیست، که باید آن را متصل کنیم.
- از طرف دیگر، وقتی قصد داریم برای اولین بار از یک MSA استفاده کنیم، هنوز هیچ سیستمی آن را نمی شناسد، و باید روی سیستم موردنظر، این MSA را نصب کرد که قابل استفاده شود.

PowerShell را با دسترسی Admin باز کرده و درج می کنیم:

New-ADServiceAccount -Name نامی دلخواه -RestrictToSingleComputer

New-ADServiceAccount -Name SA1 -RestrictToSingleComputer

حال MSA را به کامپیوتری که قصد داریم، متصل می کنیم.پس درج می کنیم:

Add-ADComputerServiceAccount -Identity نام کامپیوتر مورد نظر -ServiceAccount SA1

Add-ADComputerServiceAccount -Identity ifm -ServiceAccount SA1

حال برای اینکه از Link شدن این Service Account با کامپیوتر مورد نظر، دستور زیر را درج می کنیم:

Test-ADServiceAccount -Identity SA1

احتمالاً پیام خطایی را می دهد که می گوید این سرویس اکانت هنوز link نیست!

در حقیقت باید این Service Account را، روی این کامپیوتر نصب کرد و دوباره تست گرفت، که در پاسخ باید True بیاید:

Install-ADServiceAccount SA1

حال می توانیم به پنجره ی Services رفته و وارد Properties یک Service موردنظر شویم و در تب LogOn، سرویس اکانت SA1 را پیدا کرده و Add می کنیم، پسورد را کاملاً حذف و Apply می کنیم.

پس از Apply کردن، یک علامت $ پس از نام Service Account ظاهر می شود، که این نشانه ی یک managed Service Account است.

: Create a gMSA

پیشنیاز ساخت یک gMSA این است که از طریق ایجاد یک کلید در main Server، پشتوانه ی امنیتی را مستحکم کنیم.
این کلید امنیتی، KDS (Key Distribution Service) نام دارد.
پس دستور زیر را در PowerShell وارد می کنیم:

Add-kdsRootKey -EffectiveImmediately

در حقیقت، پس از وارد کردن این دستور، عملیات ساخت و پرداخت و آماده شدنِ کلید Root Key جهت استفاده، حدود 10 ساعت طول خواهد کشید!
اما ترفندی وجود دارد که می توان طبق آن، زمان را برای سیستم جابجا کرد، تا این کد امنیتی فوراً ایجاد شود! بصورت زیر:

Add-KdsRootKey -EffectiveTime (Get-Date).AddHours((-10))

بطور مثال برای ایجاد یک gMSA در کامپیوتر Server1 که دو کامپیوتر PC1 و PC2 بتوانند Password آنرا مدیریت کنند:

New-ADServiceAccount -name یک نام **-DNSHostName** نام **-PrincipalsAllowedToRetrieveManagedPassword** نام کامپیوتر یا محدوده ای از کامپیوترها که اجازه داشته باشند پسورد این اکانت را مدیریت کنند

در حقیقت برای DNSHostName ، نام سیستمی که می خواهیم این gMSA روی آن ایجاد شود را درج می کنیم، اما ترجیحاً بصورت نام کامل، مثل: Server.payamavar.local
برای PrincipalsAllowedToRetrieveManagedPassword ، به اشکال زیر می توان نام ها را درج کرد:

- PC1$,PC2$,PC3$: سه کامپیوتری که نام شان آمده درج علامت $ بعد از نام آنها، الزامی است.
- "Domain Computers" : تمام سیستم هایی که جزو گروه Domain Computers هستند.

New-ADServiceAccount -name g1 **-DNSHostName** Server1.payamavar.local
-PrincipalsAllowedToRetrieveManagedPassword PC1$,PC2$

حال باید gMSA ساخته شده را بر روی سیستمهایی که قرار است از آن استفاده کنند، نصب کنیم، پس در سیستم های موردنظر، PowerShell را باز کرده و درج می کنیم:

Install-ADServiceAccount -Identity نام gMSA

Install-ADServiceAccount -Identity g2

حال برای تست نصب و برقراری صحیح این gMSA در هریک از سیستم ها، درج می کنیم:

Test-ADServiceAccount -Identity g2

حال می توانیم در سیستمی که قرار است Service ای را ارائه دهد، به پنجره ی Services رفته و وارد Properties آن Service موردنظر شویم و در تب LogOn، gMSA ای که ساختیم را پیدا کرده و Add کنیم، اما گزینه ی Locations را برای آن، بر روی Entire Directory قرار می دهیم و پسورد را کاملاً حذف و Apply می کنیم.
پس از Apply کردن، یک علامت $ پس از نام Service Account ظاهر می شود، که این نشانه ی یک نوع MSA است.

نکته: برای لیست کردن تمام MSA های ساخته شده، دستور را وارد می کنیم:

Get-ADServiceAccount -Filter*

و در بخش Object-Class مشخص می شود که کدام sMSA و کدام gMSA است.

: SPN

همانطور که می دانیم، SPN یک سیستم نامگذاری یکتا برای Service ها در تمام شبکه است.
بطور مثال برای مشاهده ی سرویس هایی که روی یک کامپیوتر عضو شبکه فعال هستند، می توان وارد Properties آن در کنسول AD Users and Computers شد و در تب Attribute Editor گزینه ی servicePrincipalName را پیدا و روی آن دابل کلیک کرد.

ساختار کلی یک SPN :

<Service Class>/<Host>:<port>/<Service name>

Service Class : همان نام سرویس است، مثل نام های معروف: www، SqlServer، ldap و ....
Host : نام کامپیوتری است که میزبان Service است، یعنی این سرویس روی آن اجرا می شود که بهتر است بصورت FQDN نوشته شود.
Port : این بخش optional است.
Service Name : این بخش هم optional است.

: Register a SPN in AD DS

معمولا خود سرویس ها باید SPN خود را در AD DS ثبت می کنند.یعنی وقتی وارد Properties یک MSA می شویم، در قسمت Attribute Editor و در تنظیمات گزینه ی ServicePrincipalName، باید یک SPN برای سرویس مورد نظر درج شده باشد.
اما به دلایلی، گاهی درج نمی شود، و مجبور خواهیم بود که آن را به صورت manual انجام دهیم.

فرض کنیم که یک Service داریم به نام SV1 و یک MSA به نام SA1 که روی سیستم مورد نظر نصب و test شده است.
قصد داریم برای سرویس SV1 توسط سرویس اکانت SA1، یک SPN ثبت کنیم.
جهت ثبت SPN وارد محیط CMD می شویم.
برای این کار در ابتدا نیاز به دستور setspn داریم.اما قبل از آن، برای اینکه SPN های روی این کامپیوتر را ببینیم، می توانیم درج کنیم:

setspn -l نام کامپیوتر

setspn -s نام سرویس/ نام Host DomainNetBiosName\ نام Service Account
setspn -s SV1/ifm.payamavar.local payamavar0\SA1

نکته: البته به جای s- می توان از a- هم استفاده کرد.
نکته: می توان از درج آدرس DomainNetBiosName صرفنظر کرد و آن را ننوشت.

setspn -a SV1/ifm.payamavar.local SA1

: Create a new UPN

همانطور که می دانیم یک User، یک Name دارد که برای شناسایی آن در شبکه، از یک آدرس منحصربفرد به نام UPN که ترکیبی از این Name و DNS Suffix موجود در آن شبکه است، می باشد. مثل: Ali@payamavar.local
گاهی می خواهیم که این DNS Suffix را تغییر دهیم!
یعنی در یک شبکه، یک DNS Suffix کاملاً متفاوت داشته باشیم، طوری که به تغییر آدرس UPN نیز بینجامد.

پس در کنسول Active Directory Domains and Trust :
روی گزینه ای که به همین نام و در بالای کادر سمت چپ قرار دارد، کلیک راست کرده و وارد Properties می شویم.
حال کافی ست در کادر Alternative UPN Suffixes هر Suffix دلخواهی را Add کنیم.مثلاً : ali.com و یا jack.de و ....

حال می توانیم Suffix هر User را به هریک از Suffix هایی که ساخته ایم تغییر دهیم، یا به Properties هر User موردنظر و تب Account می رویم، و یا در هنگام ایجاد یک User، آن را تغییر می دهیم.

: Service Records

بطور معمول Service ها با شماره‌ی پورت، به همراه آدرس IP یا نام دامنه‌شان مشخص می‌شوند.
مثلاً برای دسترسی به سرویس FTP از نام دامنه‌ی example.com ، می‌توان با مرورگر ارسال کرد:
example.com:21
که در نهایت در مرحله‌ی ترجمه‌ی نام دامنه، این درخواست به‌شکل
185.143.234.5:21
یا همان [IP]:[Port] تبدیل می‌شود.

در حالت[IP]:[Port] ، در واقع یک Service روی یک رایانه‌ی مشخص در شبکه تعریف شده است که هر کاربری که بخواهد از این Service استفاده کند، باید به‌شکل دستی این آدرس IP و Port را وارد کند.

اما در حالت SRV Record ، یک Service در سطح Domain Name تعریف می‌شود. یعنی از این پس درخواست‌ها تنها به شکل Domain Name، به همراه نام Service مورد نظر و نوع Protocol آن، ارسال می‌شوند.
مثلاً همان درخواست بالا می‌تواند به شکل زیر انجام شود:
example.com ftp tcp
که این تکنیک، سرعت ارتباطات را تا حد زیادی بالاتر می برد.

Site :

در حقیقت پیشنهاد می شود که به ازای هر یک مکان فیزیکی جزء شبکه، یک **Site** منطقی در شبکه ایجاد کنیم.
با ایجاد **Site** های متفاوت، درهرصورت نیاز به **Subnet** نیز ایجاد می شود.

برخی مزایای ایجاد **Site** ها:

- **Replication Control** : می توان تعیین کرد که سایت ها در چه زمان هایی و به چه شکل با یکدیگر **replicate** شوند.
- **Assign a GPO to every single Site** :
- **Assign SRV Records** (در **DNS**) :

در حقیقت در ابتدا باید هریک از **Site** های فیزیکی، دارای یک **DC** مختص بخود بوده باشند که به شکل منطقی، عضو شبکه ی اصلی و **AD** اصلی باشند.

Create a Site :

برای ایجاد یک **Site** منطقی در **Active Directory**، در شبکه و سایت اصلی:

- در کنسول **AD Sites and Services**، در کادر سمت راست، بر روی پوشه ی **Site** کلیک راست کرده و **New Site** را می زنیم.
- گزینه ی در کادر پایین (**DefaultIPSiteLink**) را انتخاب و در نوار بالا، یک نام برای این **Site** درج و **OK** می کنیم.

البته در **PowerShell** هم می توان با دستور زیر یک **Site** جدید ایجاد کرد:

```
New-ADReplicationSite -name "نام سایت"
```

Create a Subnet :

- در همان زیرمجموعه ی پوشه ی **Site** روی پوشه ی **Subnets** کلیک راست کرده و **new Subnet** را می زنیم.
- در نوار **Prefix**، آدرس شبکه ی موردنظر را همراه با **Net Mask** آن، وارد می کنیم. (مثلاً **192.168.140.0/24**)
- در کادر پایین، سایت موردنظر را انتخاب کرده و **OK**.

Create a Site Link :

حال باید **Site** ها را به یکدیگر **Link** کنیم، که این کار را در پوشه ی **Inter-Site Transport** انجام می دهیم.
اگر سرعت ارتباط بین دو سایت زیاد نباشد یا دچار قطعی های زیاد باشد، از SMTP استفاده می کنیم وگرنه که از IP.
بطور مثال قصد ایجاد یک **Link** بین دو **Site** برحسب **IP** را داریم، پس بر روی پوشه ی **IP** کلیک راست کرده و **New Site Link** را می زنیم.
در کادر **Name** یک اسم برای این **Link** تعیین می کنیم و از کادر پایین سمت چپ، دو **Site** ای که می خواهیم **Link** کنیم را به کادر سمت راست انتقال می دهیم و **OK**.

همانطور که دیده می شود، هر **Link** دارای دو **Attribute** می باشد:

- **Cost** یا هزینه:
  برای تغییر آن باید وارد **Properties** هر کدام از **Link** ها شد.
  هرقدر که این عدد کمتر باشد، اولویت این **Link** بالاتر خواهد بود.
- **Replication Interval**:
  تعیین می کند که هر چند دقیقه یکبار این **Link** عملیات **Replication** را انجام دهد.

نکته: در زمان کار یک اداره یا سازمان، هیچ **Replication** یا **Backup** ای انجام نمی شود، پس می توان با دکمه ی **Change Schedule** این زمان ها و روزها را تعیین کرد.

- از طرف دیگر، می توان هر دو **Link** را نیز به یکدیگر متصل کرد یا بین آنها **Bridge** ایجاد کرد.
- پس درون پوشه ی **IP** کلیک راست کرده و **New Site Link Bridge** را می زنیم و دو **Link** را **Add** می کنیم.

- حال که همه چیز را تعیین و تعریف کردیم، لازم است که **DC** های موجود در شبکه را بصورت منطقی، در **Site** های ایجاد شده مختص بخود قرار دهیم که برای اینکار فقط کافی ست روی هریک از **DC** ها کلیک راست کرده و **move** و ... .

: Assign a Service Record

در حقیقت برای کار بر روی **SRV Record** ها باید به کنسول **DNS** و پوشه ی **Forward Lookup Zone** مربوط به **Domain** و سپس به پوشه ی **tcp_** مربوط به **Domain** برویم.

- روی آن کلیک راست کرده و **Other new Records** را می زنیم.
- در نوار بالا **Service Location** و سپس **Create Record** را می زنیم.
- حال می توانیم تعیین کنیم کدام **Service** با چه **Protocol** و با چه **Port** ای متصل شود.
- در نوار **Host Offering this Service** نام **DC** سایت مقصد را درج می کنیم.

: Connect Sites to eath other

اگر یکی از **Site** ها بخواهد به یک **Site** در جایی دیگر بصورت **Remote** ارتباط برقرار کند، به سه شکل می توان آن را انجام داد:

- در آن سایت **Remote**، یک **RODC** ایجاد کنیم و ارتباطات با آن را از طریق این **RODC** انجام دهیم.
- **Service Record** هایی را برای **DC** آن **Remote Site** تعریف کنیم که به این **Site** شبکه متصل شوند.
- **Subnet** هایی را برای آن **Site** دور تعریف کنیم که در محدوده ی همین **Site** حاضر در شبکه باشد.

DNS (Domain Naming System) :

وقتی یک Client درخواست ارتباط با یک IP یا یک Name را می دهد:

- ابتدا فایلی به نام Hosts که شامل یک سری Name و IP می باشد، چک می شود و اگر مقصد موردنظر در آن باشد، برطبق آن، ارتباط برقرار می شود.
  - فایل Hosts در هر سیستم، یک فایل یکتاست که قابل تغییر نیز می باشد.
  - این فایل در آدرس زیر قرار دارد:

C:\Windows\System32\drivers\etc

  - برای ویرایش آن، کافی ست آنرا با Notepad باز کنیم.
- اگر فایل Hosts شامل اطلاعاتی در مورد مقصد موردنظر نبود، حافظه ی DNS Cache سیستم چک می شود.
  - DNS Cache یک حافظه ی موقتی است که آدرس هایی که اخیراً با آنها ارتباط برقرار شده است را به اندازه ی زمان TTL، در خود حفظ می کند.
- اگر اطلاعات مقصد، در Cache هم نبود، در پایان به سوی DNS Server خواهد رفت.
  - سپس در ابتدا خود DNS Server هم در DNS Cache خودش، اطلاعات مقصد را بررسی می کند؛ که اگر در آنجا هم نبود، اطلاعات درخواستی را به ترتیب به نزدیکترین DNS Server های خارج از شبکه ارسال می کند.

چون حفظ کردن IP همه ی Object های شبکه کار ساده ای نیست، برای آنها اسم تعریف می کنیم و این اسامی همراه با IP آنها، در سرویس DNS ثبت می شوند.

Name Resolution : به تبدیل یا تفکیک کردن یک Name به IP Address یا برعکس گفته می شود.

- DNS بر اساس پورت 53 کار می کند.
- اولین پیشنیاز برای یک Replication صحیح و کامل بین DC ها، تنظیم و برقراری صحیح DNS می باشد.

وقتی در یک Client آدرس یک وبسایت را وارد می کنیم:

1. ابتدا سیستم شروع به جستجو در حافظه ی Cache مربوط به DNS خودش می کند.
2. پس اگر درون سیستم local آن را پیدا نکرد، به DNS Server شبکه، یک درخواست forward می شود.
3. اگر در DNS Server شبکه هم نبود، به Public DNS Server ای که برای آن تنظیم کرده ایم Forward می شود؛ مثلاً: 4.2.2.4
4. سپس بالاخره این وبسایت پیدا خواهد شد و به سیستم Client برخواهد گشت، اما نام این وبسایت همراه با IP آن، در تمام DNS Server هایی که بین راه بوده اند، Cache می شود.

با توجه به اینکه هر سیستم جهت ارتباط با سیستم های دیگر، نیاز به کارت شبکه دارد، پس سرویس DNS هم بر روی تنظیمات NIC، تنظیم می شود. درنتیجه به ازای هر NIC که یک سیستم دارد، می توان تنظیمات جداگانه ای را برای DNS آن نیز ثبت کرد که درنتیجه سیستم، قادر به ارتباط و استفاده از همه ی آنها خواهد بود.

دستور زیر DNS Server هایی که به کمک هریک از NIC های موجود روی سیستم پیدا می شوند را، نمایش می دهد:

```
Get-DnsClientServerAddress | select InterfaceIndex, InterfaceAlias,Address,ServerAddresses |
Format-List
```

اگر می بخواهیم ببینیم تا این لحظه مشخصات چه وبسایت هایی در حافظه ی Cache سرویس DNS سیستم Local ذخیره شده است، در cmd درج می کنیم:

Ipconfig /displaydns

- **فرض کنید آدرس وبسایت یا سیستم مقصد موردنظر تغییر کند، در نتیجه ما به هرشکلی که قصد دسترسی به آن مقصد را داشته باشیم، نمی توانیم! چون هنوز آدرس قبلی در سیستم DNS مان ثبت است! پس باید حافظه ی Cache سیستم مان را پاک کنیم. برای این کار دستور زیر را وارد می کنیم:**

Ipconfig /flushdns

- **اگر در شبکه، فقط یک DC وجود داشته باشد، می توانیم اولین آدرس DNS روی NIC همه ی اعضای شبکه، باید آدرس IP این DC باشد، و برای دومی، می توان یک DNS Address معروف و جامع مثل 8.8.8.8 را وارد کرد.**
- **اگر دو DNS Server در شبکه موجود باشد، دومین DNS همه ی اعضای شبکه را برابر با IP سیستم DNS دوم قرار می دهیم.**

:Implement a DNS Server

در حقیقت به محض نصب کامل اولین Role که AD DS می باشد، الزاماً Role مربوط به DNS را هم نصب می کنیم، که فعال شده و در Server manager قابل دسترسی خواهد بود.

برای نصب DNS Server می توان از Add Roles and Features عمل کرد و یا به یکی از روش های زیر:

نصب تحت PowerShell	Install-WindowsFeature DNS -IncludeAllSubFeature -IncludeManagementTools
حذف تحت PowerShell	Uninstall-WindowsFeature DNS -IncludeAllSubFeature -IncludeManagementTools
نصب تحت cmd	Dism /online /enable-feature /featurename:DNS-Server-Core-Role
حذف تحت cmd	Dism /online /disable-feature /featurename:DNS-Server-Core-Role
دریافت دستورات PowerShell	gcm -Module DnsServer

وقتی که نقش DNS را نصب کردیم، وارد کنسول آن می شویم تا پیکربندی های اولیه را انجام دهیم:
در سمت چپ، روی گزینه ای با نام کامپیوتر Server کلیک راست کرده و Properties را می زنیم.

➢ تب Interfaces :
اولین نکته ای که در این Tab وجود دارد این است که در کادر پایین، می بینید که این کامپیوتر به ازای NIC هایی که دارد، چه آدرس هایی را دارا می باشد.
با تیک زدن هریک از آنها می توانید مشخص کنید که برای کدام یک از کارت شبکه ها و تحت کدام ورژن از IP، عمل Name Resolution انجام شود و برای کدام یک نشود؛ و یا اینکه می توان All IP را بزنیم!

➢ تب Forwarders :
در حقیقت آدرس DNS Server های دیگر تعریف شده برای سیستم را می بینیم.
می دانیم که اگر IP یا Name یک مقصد در Cache و Host سیستم DNS Server موجود نباشند، این DNS Server باید یک درخواست به یک DNS Server دیگر که می تواند Public یا عضو شبکه ی خودمان باشد، ارسال کند، که به آنها Forwarder گفته می شود.
پس در این تب باید Forwarder ها را مشخص کنیم. روی Edit زده و IP آنها را یکی یکی درج می کنیم.
اضافه یا حذف Forwarder از طریق PowerShell مثلاً برای گوگل:

```
Add-DnsServerForwarder 8.8.8.8
Remove-DnsServerForwarder 8.8.8.8
```

اگر بخواهیم ببینیم تا این لحظه مشخصات Name و IP چه وبسایت هایی در حافظه ی Cache مربوط به DNS Server سیستم تان ذخیره شده است، در PowerShell درج می کنیم:

```
Show-DnsServerCache
```

برای اینکه این حافظه ی Cache مربوط به DNS Server را پاک کنید از دستور زیر در PowerShell استفاده کنید:

```
Clear-DnsServerCache
```

:Advanced View

برای مشاهده ی برخی تنظیمات Zone ها، مثل TTL و ... باید در منوی بالای کنسول DNS، روی View کلیک کرده و Advanced را فعال کرد.

: Conditional Forwarder

فرض کنید که بخواهیم برای یک سری از وبسایت ها، یک **Forwarder** خاص را تعیین کنیم.

- در زیرمجموعه ی آبجکت **Server** در کنسول **DNS**، وارد پوشه ی **Conditional Forwarders** می شویم.
- روی آن کلیک راست و **New** را می زنیم.
- در نوار **DNS Domain**، نام وبسایت موردنظر را و در کادر پایین، آدرس **Forwarder** ها را درج می کنیم.

➢ جهت انجام آن از طریق **PowerShell**:

```
Add-DnsServerConditionalForwarderZone www.imdb.com 4.2.2.4
```

➢ جهت مشاهده ی **Conditional Forwarder** های تعریف شده به کمک نام سیستم **Domain Controller**:

```
Get-DnsServerForwarder -ComputerName PAYAMAVAR
```

➢ جهت افزودن یک **Conditional Forwarder**:

```
Add-DnsServerForwarder -IPAddress 192.168.1.1
```

➢ جهت تغییر یک **Conditional Forwarder** (جایگزین کردن مقادیر جدید، طوری که قبلی حذف می شود):

```
Set-DnsServerForwarder -IPAddress 8.8.8.8, 8.8.4.4
```

➢ جهت حذف یک **Conditional Forwarder**:

```
Remove-DnsServerForwarder -IPAddress 192.168.1.1
```

: Root Hint

در حقیقت اگر هیچ Forwarder ای را در DNS Server تعریف نکنیم، DNS هنوز هم می تواند به Root Server های بزرگ شبکه ی اینترنت دسترسی داشته باشد.

Root Server ها از قبل بصورت پیشفرض، در DNS و در مکانی به نام Root Hints ثبت و تعریف شده اند.

- وقتی که DNS Client درخواست دسترسی یک Name یا IP را به DNS Server ارسال می کند، آن را در یک پیام recursive (یکطرفه) می فرستد.
- درخواستی که به Forwarder ارسال می شود نیز، یک پیام recursive است.
- اگر Forwarder ای تعریف نشده باشد، **یک پیام iterative** به Root Server ارسال می شود.

نکته: Root Server ها معمولاً فقط آدرس Server های پسوندهای دامنه ی معروف مثل .com و ... را می شناسند.

- پس آدرس سروری که دامنه های مثلاً .com در آن وجود دارند، توسط **یک پیام iterative** به DNS Server ما بر می گردند.
- به هرحال Server ای که دارای دامنه ی .com است، یا خودش مقصد را معرفی می کند و یا آدرس Server منطقه ای که آن مقصد مورد نظر، در آنجا حضور دارد را طی **یک پیام iterative** به DNS Server بر می گرداند.

- به عمل ارسال تقاضا از Client به سمت Server ، DNS Query گفته می شود.
- ارتباط DNS Server با همه ی Root Hint ها (که پسوندهای دامنه را شناسایی می کنند)، بصورت پیام های iterative می باشد، که به هریک از آنها، Iterative Query گفته می شود.

- Recursive Query به این معناست که DNS Server حق ندارد جهت پاسخ به DNS Query، کلاینت را به Server ای دیگر ارجاع دهد، بلکه باید خودش پاسخ آن را پیدا کرده و پس بفرستد.
  به این صورت که Recursice فقط یکطرفه است، یعنی فقط ارسال می شود و باید منتظر پاسخ ماند.

برای modify یا ایجاد تغییرات بر روی Root Hint :

روش اول: در کنسول DNS، آبجکت DC را انتخاب کرده و در کادر سمت راست، وارد Properties گزینه ی Root Hints می شویم.

روش دوم: وارد Properties خود گزینه ی DC شده و به تب Root Hints می رویم.

روش سوم: به مسیر درایو C، پوشه ی Windows و سپس System32 رفته و در پوشه ی DNS ، فایل Cache.dns را با Notepad باز می کنیم.

همانطور که می بینیم، به راحتی می توان IP هایی را همراه با نام آنها، به عنوان Root Hint اضافه کرد، اما برای اضافه کردن از طریق P.Shell:

```
Add-DnsServerRootHint ifm.payamavar.local  آدرس IP
```

نکته: اگر هیچ Forwarder ای نداشته باشیم و همه ی Root Hint ها هم حذف شده باشند یا فقط بر اساس ورژن 6 کار کنند، مجبور خواهیم بود بطور موقت یک Forwarder مثل 8.8.8.8 را ثبت کنیم، و سپس در تب Root Hint ها، Root hint هایی که فقط با ورژن 6 کار می کنند را باز کرده و Resolve کنیم.

Zone :

Zone نامی ست که به Database مربوط به Name ها و IP های شبکه گفته می شود.

از لحاظ تغییرپذیری یا قابلیت خواندن، Zone ها به دو دسته تقسیم می شوند:

- Primary : هردو قابلیت Read و Write را دارد.
- Secoundary : فقط قابلیت Read دارد.

در حقیقت برای شبکه ی یک سازمان یک Primary Zone تعریف می کنیم و سپس اطلاعات این Primary Zone را به یک Secoundary Zone که در یک DMZ قرار دارد، می دهیم.

از لحاظ کارکرد هم دو نوع Zone وجود دارد:

- Forward Lookup Zone : منطقه ای که در آن Name ها به IP Address تبدیل می شوند.
- Reverse Lookup Zone : منطقه ای که در آن IP Address ها به Name ها تبدیل می شوند.

به طور پیشفرض، همیشه هیچ Reverse Lookup Zone ای نداریم، اما دو Forward Lookup Zone داریم که هر دو Primary هستند:

- _msdcs.payamavar.local مربوط به خود Active Directory است.
- دیگری به نام خود Root Damain است و همه ی پیکربندی های DNS شبکه، در آن قرار می گیرند.

انواع رکوردهایی که قابل ثبت شدن در Zone ها می باشند:

- A : عملیات Name Resolution را برای IP v4 انجام می دهد.(FQDN to an IPv4)
- AAAA (Quad A): عملیات Name Resolution را برای IPv6 انجام می دهد.(FQDN to an IPv6)
- Cname یا Canonical Name (Alias): یک نام مستعار برای یک Name است، که می تواند به دلایل امنیتی باشد.
- NS (Name Server): مکان اصلی ذخیره سازی Name ها و IP هاست.هر Zone می تواند چندین NS داشته باشد.
- PTR (Pointer): نوع رکورد مربوط به عملیات Reverse است.
- MX (Mail Exchanger): نوع رکورد مربوط به Mail Exchanger هاست.
- SRV : نوع رکورد مربوط به Server هاست.
- SOA (Start of Authority): اولین رکوردی است که به صورت خودکار در Zone ایجاد شده و اطلاعات خودِ Zone در آن وجود دارند.

از لحاظ مکان ذخیره سازی، Zone ها به دو دسته تقسیم بندی می شوند:

- **Active Directory Integrated Zone :**

اطلاعات این Zone، درون Database اکتیودایرکتوری ذخیره می شود.به عبارت دیگر Active Directory از اطلاعات این Zone محافظت می کند.

- **Standard Zone :**

اطلاعات این Zone، در مسیر زیر ذخیره می شوند.

C:\windows\system32\dns\alireza.com.dns

همانطور که می بنید اطلاعات این zone در سیستم عامل ویندوز ذخیره می شود از لحاظ امنیت و دسترسی، نسبت به بالایی ضعیف تر هست.

TTL (Time To Live):

این اصطلاح به دو قابلیت اشاره دارد، یکی در ارتباطات بین شبکه ای، و یکی در ارتباطات مربوط به DNS.

TTL in Network :

TTL در شبکه به زمان زندگی یک بسته در هنگام انتقال بین دو یا چند سیستم گفته می‌شود.

در هنگام ارسال یک Packet، زمان زندگی یا TTL برای آن در نظر گرفته می شود و پس از اتمام آن، بسته به طور کل از بین خواهد رفت.

برای دیدن TTL یک بسته می‌توان از دستور Ping استفاده کرده و متوجه مقدار TTL بسته ی ICMP گردید.

مقدار TTL برای این بسته 64 است و این به این معناست که این بسته بعد از رد شدن از 64 نود از بین می‌رود.

- بصورت پیشفرض، سیستم‌های پایه ی لینوکس، بسته را با مقدار 64 و در سیستم‌های پایه ی ویندوز با 128 ارسال می‌کنند.

نکته : مقدار TTL پس از گذر هر روتری در مسیر به صورت پیشفرض کم خواهد شد مگر آنکه تنظیماتی در روتر انجام شده باشد که TTL کسر نکند.

TTL in DNS :

TTL در DNS به همان معنای زمان زندگی است، اما نه زندگیِ یک بسته!

هنگامی که شما نام دامنه‌ای را در نوار آدرس مرورگر خود وارد می‌کنید، توسط DNS نام دامنه ی شما به IP برمی‌گردد و این آدرس IP و دامنه در Cache سیستم شما ذخیره خواهند شد تا در دفعات بعد، نیاز به درخواست به سمت DNS نداشته باشیم و سرعت افزایش یابد.

TTL در DNS به مقدار زمانی گفته می شود که آن آدرس IP و دامنه برای شما Cache می مانند.

در TTL شبکه، مقدار TTL تنها یک عدد است اما TTL در DNS بر مبنای ثانیه تنظیم شده و بر هر حسب ثانیه نیز عمل می‌کند.

به عنوان مثال اگر TTL یک دامنه بر روی مقدار 86400 باشد ، بدین معناست که مشخصات آدرس IP و دامنه به مدت یک روز روی سیستم شما کاربر، Cache خواهند شد.

اگر دستور **ipconfig /displaydns** را بزنیم، اطلاعات کامل هریک از Record های موجود در DNS سیستم را می بینیم که زمان Time to Live را نیز نشان می دهد.

به رکوردهایی که اطلاعاتی برایشان ثبت نشده است، و در پاسخ دستور بالا، Name does not exist را نشان می دهند، **Negative cache** گفته می شود.

و به رکوردهایی که در پاسخ به دستور بالا، اطلاعاتی را پاسخ می دهند، **Positive Cache** یا **Positive Response** گفته می شود.

مقدار TTL برای Negative cache ها بطور default برابر است با 300 ثانیه یا 5 دقیقه و برای Positive Cache ها، برابر است با 86400 ثانیه، یا یک روز.

: NSLookup

اطلاعاتی در مورد Name و IP Address یک وبسایت می دهد؛ همراه با Cname های آن :

nslookup www.Website.de

آدرس های ورژن 4 یا 6 وبسایت موردنظر را می دهد، همراه با Cname های آن:

nslookup -type=A ویا AAAA www.Website.de

اطلاعاتی در مورد Name Server یک وبسایت می دهد؛ مثلاً Cname های آن و ...:

nslookup -type=ns www.Website.de

برای دریافت اطلاعات Mail Exchanger (MX records) یک Domain یا یک Website:

روش اول:

nslookup -type=mx www.Website.de

روش دوم:

اینتر- Nslookup و یا اینتر- Nslookup – 4.2.2.4

اینتر- set q=mx

اینتر- DOMAINNAME

برای دریافت آدرس DNS Server یک Domain یا یک Website:

اینتر- Nslookup و یا اینتر- Nslookup – 4.2.2.4

اینتر- DOMAINNAME

آدرس های ورژن 4 و 6 وبسایت را همراه با TTL آنها بصورت منظم نشان می دهد:

Resolve-dnsname www.Website.de

Create a Zone :

در حقیقت ما باید یک Object داشته باشیم که بخواهیم برای آن یک Zone ایجاد کنیم. مثلاً یک Server عضو شبکه یا … .

برای Froward Lookup Zone **:**

- بر روی **Forward Lookup Zone** کلیک راست کرده و **New Zone** را می زنیم.
- **Primary** را انتخاب می کنیم و در پایین این تب:
- اگر تیک **Store Zone in Acive Dir.** را فعال کنیم، تبدیل به یک **Active Directory integrated Zone** خواهد شد، یعنی یک نسخه از این **Zone** در همه ی **DC** های شبکه هم ایجاد و مدام با آن **replicate** و **update** می شود که در تب بعد، باید تعیین کنیم که اطلاعات این **Zone** به چه شکل **Replicate** شوند، که به آن **Replication Scope** گفته می شود:
  - با تمام **DNS Server** هایی که بر روی تمام **DC** های تمام محیط این **Forest** هستند.
  - بطور معمول این را می زنیم: **با تمام DNS Server هایی که بر روی تمام DC های تمام محیط این Domain هستند.**
  - با تمام **DC** هایی که در تمام محیط این **Domain** هستند.
- اما اگر گزینه ی **Store Zone in Acive Dir.** را غیرفعال کنیم، این **Zone** تنها در همین **DC** ایجاد می شود.

- **Name Server** موردنظر را بصورت کامل می نویسیم، مثلاً: **dc1.payamavar.local**
- در تب **Dynamic Update** یکی از گزینه های **Allow** را می زنیم. پس باید با مفهوم **Dynamic Update** آشنا شویم: یعنی هر کامپیوتر را مجبور می کنیم که به صورت اتوماتیک برای خودش داخل **Zone**، یک **A-Record** ثبت کند یا خیر!
- در هر حالت تیک گزینه **Allow both…** را می زنیم.
  - **Secure** به **Client** هایی می گویند که عضو **AD** هستند.
  - **Non-Secure** به **client** هایی می گویند که عضو **AD** نیستند.
- **Next** را زده و در انتها **Finish**!

Zone ای که ایجاد می شود به صورت پیش فرض دو رکورد داخل آن ایجاد می شود.

- اولی **SOA** که کار آن محل شروع **Zone** را نشان می دهد و دومی **NS** (**Name Server**) است که به **Client** هایی که وارد این **Zone** می شوند اعلام می کند سوالاتشان را از چه کسی (**Server** ای) بپرسند.

در PowerShell :

برای ایجاد Zone :

```
Add-DnsServerPrimaryZone -Name memser.payamavar.local -ReplicationScope Domain
```

برای ایجاد یک رکورد از نوع A به نام PC1 درون Zone ای به نام payamavar.local:

```
Add-DnsServerResourceRecordA -Name "PC1" -ZoneName "payamavar.local" -IPv4Address
"192.168.139.150"
```

بطور معمول اگر وارد **Properties** و تب **Name Server** مربوط به **Zone** ها شویم، باید **Server** های شبکه **Link** باشند.

اگر بخواهیم یک **Server** دیگر را در آنجا **Add** کنیم، کافی ست پس از فشردن **Add**، آدرس **FQDN** آنرا وارد کنید و یکبار آنرا **Resolve** کنید که **IP** آن هم اضافه شود، و **OK**!

- برای اینکه فوری این عملیات در **DNS Server** دوم هم ایجاد شود، کافی ست بر روی این **Zone** در **DNS Server** دوم، کلیک راست کرده و **Transfer New Copy of Zone from Master** را بزنیم.

نکته: برای اینکه Record های جدید بطورمستقیم در یک DNS Zone ثبت نشوند، dynamic Update آن را روی secure only قرار می دهیم.

: Secondary Zone

حال که یک **Primary Zone** داریم، می خواهیم یک نسخه ی **Secoundary** از آن ایجاد کنیم.
Secondary Zone باید در یک **Server** دیگر راه اندازی شود.

- نمی توان از یک **Primary Zone**، در **Forward Lookup Zone** خودش، یک **Secondary Zone** ایجاد کرد!

نکته: اگر بخواهیم تنظیمات **DNS** یک **Server** دیگر را در همین **Server** جاری، همزمان داشته باشیم، در کنسول **DNS** بر روی نام **DC** کلیک راست کرده و **Connect to DNS Server** را زده و آدرس **UNC** کامپیوتر آن **Server** را وارد می کنیم.

با استفاده از **Secondary Zone** می توانیم حجم بیش از اندازه ی ترافیک را از روی **Server** اصلی برداریم.
اگر **Server** اصلی از کار بیفتد، **Server** شامل **Secondary Zone**، شروع به سرویس دهی می کند تا **Server** اصلی به شبکه بازگردد.

نکته: اگر درون **Forward Zone** سرور دوم هم یک نسخه ی **Primary** از **Forward Zone** مورد نظر وجود داشته باشد، نمی توان نسخه ی **Secoundary** آن را ایجاد کرد.

پس در بخش **DNS Server** دوم، وارد ویزارد ایجاد **Zone** شده و نوع **Secoundary** را انتخاب کرده و برای **Name** می توانیم **Browse** را زده و آبجکت سرور **Primary** ای که در **Server** اول وجود دارد را انتخاب کنیم.

برای **IP** آن، باید **IP** سرور اصلی (سیستمی که **DNS Server** اصلی روی آن تعریف شده است) را وارد کنیم، که معمولاً همان **Root DC** است.
تذکر: اگر پس از وارد کردن **IP**، خطای **Validation Error** داد، می توان فعلاً از آن گذر کرد و تمام!
(اگرچه این خطا احتمالاً به دلیلِ نداشتن **Permission** است.)

اما اگر پس از نصب **Security Zone** با کلیک بر روی آن، باز هم خطای دسترسی داد، باید اجازه ی دسترسی به آن را در سروری که بر روی آن قرار دارد، فعال کنیم.

- پس در **DNS** میزبان آن، وارد **Properties** مربوط به **Primary Zone** آن می شویم.
- در تب **Zone Transfers** ، گزینه ی **Allow Zone transfers** را فعال می زنیم.
- یکی از زیرگزینه های آن را انتخاب و تنظیم می کنیم و **OK**!

در تب Zone Transfer تعیین می کنیم که کدام Zone های دیگر، بتوانند اطلاعات این Zone را گرفته و نشان دهند.
در حقیقت تعریف کردن این تب، فقط برای **Primary Zone** ها معنا می دهد، مگر اینکه بخواهیم یک **Secondary Zone** دیگر از این **Zone** که خودش هم **Secondary** است، اطلاعات دریافت کند!
معمولاً برای **DC** اصلی شبکه، برای **Primary Zone** اصلی آن، در این تب، آدرس **Zone** های **Secondary** در **DC** های دیگر (که نمی خواهیم تغییری در **DNS** ایجاد کنند، فقط دسترسی داشته باشند) و یا اگر قصد داشته باشیم تا این **Zone** در یک **DC** دیگر هم قابل کنترل باشد، نام آن **DC** را درج می کنیم.

در تب Name Server تعیین می کنیم که این Zone اطلاعاتش را از کدام DC یا در حقیقت از کدام DNS Server دریافت کند.
در حقیقت در این تب، می توانیم آدرس همه ی **DC** های دیگری که نسخه ی **Primary** از این **Zone** را دارند درج کنیم، اما به روز کردن اطلاعات یک **Primary Zone** توسط یک **Secondary Zone** بی معنی است!

حال برای اعمال این تغییر، بر روی Security Zone که دچار خطا شده است، کلیک راست کرده و Transfer from Master را می زنیم.

ما می توانیم به Zone ها هم nslookup کنیم، که فقط نام کامل آنها را پاسخ می دهد.

nslookup memser.payamavar.local

اما اگر در یک Zone، یک Host بدون Name ایجاد کنیم، این به آن معنا خواهد بود که این Zone مربوط به سیستمی به نام خود این Zone است، پس با nslookup به آن، آدرس این Host را می دهد.

برای nslookup کردن به Host های درون یک Zone، باید نام کامل آنها را درج کرد، مثلاً:

nslookup PC1.memser.payamavar.local

برای Reverse Lookup Zone **:**

- بر روی Reverse Lookup Zone کلیک راست کرده و New Zone را می زنیم.
- Primary را انتخاب و تیک .Store Zone in Acive Dir را فعال می کنیم.
- IPv4 را انتخاب می کنیم.
- آدرس Network ID ای که Zone مورد نظر در آن قرار دارد را وارد می کنیم.
- تعیین می کنیم که اطلاعات این Zone به چه شکل Replicate شوند!
- تمام!
- همانطور که گفتیم یک رکورد وجود دارد به نام PTR یا Pointer که مربوط به Reverse Zone هاست.

در حقیقت، هر رکورد PTR، یک IP است که اشاره دارد به یک Name.

برای ایجاد یک Pointer :

- در کادر Reverse Zone، کلیک راست کرده و New PTR را می زنیم.
- می توانیم IP سیستم موردنظر را وارد کنیم، و یا اینکه نام آن را درج یا Browse کنیم.

نکته: ما می توانیم در Forward Lookup Zone، یک Name جدید را همراه با IP آن طوری تعریف کنیم که بطورخودکار، PTR آن هم در Reverse Zone مربوطه ایجاد شود.

نکته: اگر Reverse Zone مربوط به Network ID یک آدرس IP، در Reverse Lookup Zone موجود نباشد، هیچ PTR Record ای برای آن ایجاد نمی شود! پس باید ابتدا یک Reverse Zone برای آن ایجاد کرد.

کافی ست در بخش Forward Lookup Zone کلیک راست و New Host را بزنیم و فقط نام کامپیوتر مقصد و IP آنرا وارد کنیم، و البته تیک گزینه ی (Created associated pointer (PTR را بزنیم.

برای اطلاع از وضعیت Zone ها، در PowerShell درج می کنیم:

```
Get-DnsServerZone
```

برای دریافت همه ی رکوردهای یک Zone :

```
Get-DnsServerResourceRecord -ZoneName payamavar.local
```

برای دریافت همه ی A Record های یک Zone :

```
Get-DnsServerResourceRecord -ZoneName payamavar.local -RRType A
```

به هر DNS Server ای که میزبان یک Zone باشد، Authoritative DNS Server گفته می شود.

هرگاه در پاسخ دستور nslookup، خطای Non-authoritative answer را داد، تنها به این معنی است که این پاسخ را از درون Cache خود سیستم ارائه داده است. برای رفع این خطا باید Cache را پاک کنید و دوباره nslookup بگیرید.

Round Robin :

برای اینکه فشار بارکاری یک **Server** را کاهش دهیم، یا به عبارتی، **Work Load** را بین چندین **Server** پخش کنیم، می توانیم توسط تکنیک **Round Robin**، **IP** های مختلفی را برای یک **Name** تعیین کنیم.
Round Robin به صورت گردشی، **IP** هایی که برای یک **Name** تعیین شده را به آن اختصاص می دهد.

اما در ارتباطات با وبسایت هایی که **Session base** هستند و کاربر باید با آنها یک ارتباط یکطرفه ی مستقیم برقرار کند، مثل سامانه های بانکی، نباید از سیستم **Round Robin** استفاده کرد!

برای فعالسازی یا غیرفعالسازیِ آن، باید روی **Server** مورد نظر، کلیک راست کرده و **Properties** را زد و در تب **Advanced**، گزینه ی **Enable Round Robin** را فعال یا غیرفعال کرد.

در واقع با استفاده مکانیزم **Round Robin**، اگر دو عدد **Web Server** مشابه داشته باشیم، **DNS Server** رکوردهای آنها را که دارای آدرس های **IP** غیرمشابه می باشند، در خود خواهد داشت.
فرض کنید **Client** ها به این **Web Server** درخوست ارسال کنند. اولین درخواست برای **Server** اول و دومین درخواست به **Server** دوم ارسال خواهد شد.
در واقع سرویس **Round Robin** به نوعی برای ما **Load Balancing** در سطح **DNS Server** ایجاد می کند.
به رکوردهای زیر دقت کنید، هر کدام دارای یک آدرس **IP** متفاوت در یک **DNS Server** هستند اما با قابلیت **Round Robin** درخواست اول به سمت آدرس **IP** شماره **192.168.1.100** و درخواست دوم به سمت آدرس **IP** به شماره **192.168.1.200** برای برگرداندن اسم **www.pa.com** ارسال خواهد شد:

```
A Record : www.pa.com = 192.168.1.100
A Record : www.pa.com = 192.168.1.200
```

و یا اگر واقعاً دو **Web Server** با نامی یکسان و با **IP** های متفاوت داشته باشیم هم این قابلیت، کارآمد است.

راه اندازی Round Robin:

فرض کنید دو سرور به نام های **IFM1** و **IFM2** داریم که همه ی تنظیمات **DNS** شبکه، بر روی **IFM1** قرار دارند.

- در **Forward Lookup Zone** مربوط به **IFM1**، وارد **Properties** مربوط به **Forward Zone** سرور اصلی شده و **Zone transfer** را به فقط **IFM2** انتقال می دهیم.
- در همان **Forward Zone** مربوط به **IFM1**، وارد **Properties** رکورد **SOA** شده و در تب **Name Server**، سرور **IFM2** را **Add** می کنیم.
- در **Reverse Lookup Zone** مربوط به **IFM1**، وارد **Reverse Zone** مربوط به **IP** سرور اصلی شده و وارد **Properties** رکورد **SOA** شده و در **Name Server** ، سرور **IFM2** را **Add** می کنیم.
- در تنظیمات همان **SOA**، **Zone transfer** را به فقط **IFM2** انتقال می دهیم.
- حال در کنسول **DNS Server** مربوط به **IFM2**، ابتدا یک **Secoundary Lookup Zone** از سرور اصلی و سپس یک **Secoundary Reverse Zone** ایجاد می کنیم.
- حال **PTR** ها و رکوردهای **A** یا **AAAA** بی اهمیت را در **IFM1** حذف کرده و بر روی **Zone** های **forward** و **Reverse** سرور دوم، کلیک راست کرده و **Transfer new Copy of Zone from Master** را می زنیم.
- حال به سادگی در **Forward Zone** مربوط به **IFM1**، چند **Host** با **Name** های یکسان (مثلاً **S1**) و **IP** های متفاوت (با **Network ID** های یکسان) ایجاد می کنیم.

حال اگر در **PowerShell** دستور **nslookup S1** را درج کنیم، می بینیم که هرسه **IP** به آن اختصاص داده شده اند.

Netmask Ordering :

زمانی به قابلیت Netmask Ordering نیاز پیدا خواهیم کرد که قابلیت Round Robin فعال شده باشد.

رکوردهای زیر را در نظر بگیرید:

```
A Record : www.pa.com :192.168.1.100
A Record : www.pa.com :192.168.1.200
A Record : www.pa.com :172.16.1.100
A Record : www.pa.com :172.16.1.200
A Record : www.pa.com :85.146.23.77
```

همانطور که مشاهده می کنید ما 5 عدد A Record در DNS Server داریم که همه ی آنها به www.pa.com اشاره می کنند ولی آدرس های IP هر کدام از آنها متفاوت است.

تصور کنید یکی از کارت شبکه های این DNS Server به شبکه ی داخلی متصل است و کلاینتی از این شبکه ی داخلی دارای آدرس IP به شماره ی 192.168.1.50 است و درخواست پیدا کردن آدرس IP وب سایت www.pa.com را به این DNS Server می فرستد.

DNS Server متوجه می شود که درخواست Client ما از آدرسی ارسال شده است که با دو عدد از رکوردهای موجود برای این Name در DNS Server تشابه دارد!

پس در اینجا قابلیت Netmask Ordering به DNS Server می گوید که در پاسخ به این کلاینت باید رکورد www.pa.com با آدرسIP به شماره ی 192.168.1.100 یا 192.168.1.200 را بازگردانی کند.

پس فقط با یکی از این دو رکورد برای Client های داخلی پاسخ می دهد.

DNS Delegation :

با ساخت اولین Domain، در DNS Server، یک Zone مربوط به آن هم به صورت خودکار ساخته می شود.

درحقیقت پس از ایجاد Child DC ها، برای DNS Server آنها، می توان برای هریک از آنها، یک Zone ایجاد کرد، که در این روش، ترافیک شبکه سنگین می شود.

یک روش دوم هم هست، که می توان بر روی Forward Lookup Zone اصلی شبکه، کلیک راست کرده و New Domain را زد، که به این شکل، همه ی ویژگی های شبکه ی اصلی، بطورخودکار به Child Domain ها هم منتقل می شوند.

اما در روشی دیگر، می توان Child DC ها را به DNS Server مربوط به main DC وکالت داد یا delegate کرد.

1. **در DNS Server مربوط به یک سیستم Child Domain به نام memser.payamavar.local، یک Primary Forward lookup Zone ایجاد می کنیم، طوری که برای نام آن، نام کامل Root Domain را به عنوان پسوند، به آن اضافه می کنیم. مثلاً به نام Ent.payamavar.local ، با این تفاوت که don't allow dynamic updates را انتخاب می کنیم.**
2. **یک رکورد A (Host) برای آن به نام مثلاً Server3 و یک IP دلخواه تعریف می کنیم.**

حال اگر در main DC به Zone به نام ent.payamavar.local و یا به Server3 یکبار nslookup یا Ping کنیم، هیچ نتیجه ای نمی دهد!

چون باید این Zone را ابتدا به سرور اصلی شبکه، delegate کنیم:

3. **در DNS Server سرور اصلی، بر روی Zone مربوط به Root DC کلیک راست کرده و new Delegation را می زنیم.**
4. **برای delegated domain فقط درج می کنیم : ent**
5. **سپس FQDN مربوط به سروری که در کنسول DNS آن، primary Zone ای بنام ent.payamavar.local را ایجاد کردیم، درج می کنیم: memser.payamavar.local**

حال اگر nslookup بگیریم، مشخصات ظاهر خواهند شد، که البته شامل یک Error بی اهمیت نیز می باشد!

بدینصورت، هربار که یک درخواست به سرور اصلی شبکه یعنی Payamavar.local وارد شد که نیاز به دسترسی به Zone به نام ent.payamavar.local داشت، به سادگی بطور خودکار، متصل خواهد شد.

: Stub zone

فرض کنید مثلاً یک Conditional Forwarder را تعریف کرده ایم!
فرض کنید Forwarder و یا وبسایتی که Forwarder را به آن نسبت داده ایم، دچار تغییرات Name یا IP می شود، که قابل دسترسی نخواهد بود. پس مجبور خواهیم بود که به صورت دستی تغییرات را اعمال کنیم که باز هم وقتگیر خواهد بود.

پس در اینجا، می توانیم یک Stub Zone، در داخل شبکه ی خودمان تعریف کنیم.
Stub Zone بطور Dynamic، مدام اطلاعات آن دامین مربوط به آن وبسایت را دریافت می کند تا همیشه از بروز تغییرات مقصد موردنظر، مطلع باشد و کاربران مشکلی برای دسترسی به آن نداشته باشند.

Stub Zone یک کپی از Primary Zone شبکه ی مقصد است که فقط name server و رکوردهای SOA را ذخیره می کند.
این ویژگی برای زمانی مناسب است که شما با یک سازمانی همکاری می کنید، در این حالت به جای ایجاد secondary zone ، کافی است یک stub zone از سرورآن DNS ایجاد کنیم، و هنگامی که Client ها، DNS Server را کوئری می کنند، می توانند به بروزترین موقعیت رکورد، توسط stub zone دسترسی داشته باشند.

برای بررسیِ Stub Zone:

- در یکی از Server ها (مثلاً memser.payamavar.local)، یک Primary Zone ایجاد می کنیم و تیک Store the Zone in Active Directory را غیرفعال می کنیم. مثلاً به نام: Example.com
- برای آن، دو رکورد A، با نام های دلخواه و با IP های متعلق به شبکه ی جاری تعیین می کنیم.
- حال وارد Properties رکورد SOA و تب Name Server می شویم.
- یک Name Server بنام مثلاً Memser.example.com و با یک IP متعلق به شبکه ی جاری، اضافه می کنیم.

نکته: دقت داشته باشید که در پوشه ی Forward Lookup Zone اصلی شبکه، در حال حاضر هیچیک از Forward Zone های سرور Memser.payamavar.local وجود نداشته باشند، و اگر باشند، باید آنها را حذف کنید.

- حال بر روی Forward Lookup Zone اصلی شبکه (مربوط به payamavar.local) کلیک راست کرده و New Zone را می زنیم، و Stub Zone را انتخاب کرده و تیک Store the Zone in AD را فعال نگه می داریم.
- برای Zone Name همان Example.com را انتخاب می کنیم.
- IP مربوط به سروری که Example.com را در Forward Lookup Zone های آن ایجاد کردیم (یعنی memser.payamavar.local) را وارد کرده و تیک Use the above servers to create a l.. را فعال می کنیم.

حال با اینکه در Forward lookup Zone مربوط به Example.com موجود در سرور اصلی، هیچیک از رکوردهای A تعریف نشده اند، اگر در CMD به Name یکی از رکوردهای A، دستور Lookup را بزنیم، جواب خواهیم گرفت.

Create a CName :

از ویندوز Server 2008 به بعد، به جهت کمک به سازمان‌ها به منظور حذف WINS و جایگزینی آن با سرویس‌های مبتنی برDNS ، از Zone های جدیدی با نام GlobalName Zone پشتیبانی می شود که به آن Single Label Name نیز گفته می شود.
این Zone ها دقیقا مانند WINS به صورت Single Label هستند و در واقع می‌توانید آن‌ها را نام‌های DNS بدون پسوند، مثل com. و net. در نظر بگیرید.
برخلاف WINS، GlobalName Zone ها برای پشتیبانی از شبکه‌های Peer-to-Peer و Name Resolution ایستگاه های کاری، مناسب نیستند و از به روزرسانی خودکار DNS (DNS Dynamic Update) پشتیبانی نمی کنند.
GlobalName Zone ها برای کار با Server ها طراحی شده‌اند.
پس چون از نوع Dynamic نیستند، مدیر شبکه باید به صورت دستی رکوردهای آن‌ها را به Zone های خود اضافه کند.
در اکثر سازمان‌ها، سرورها Static IP دارند و این مورد با طراحی GlobalName Zone ها همخوانی کامل دارد.

برای اینکه، جهت فراخوانیِ رکوردهای A موجود در Server اصلی، بجای درج کامل FQDN آن، با یک CName آنها را فراخوانی کنیم:

- قابلیت Global Name Zone را فعال می کنیم.
- یک Global Zone ایجاد می کنیم.
- سپس رکوردهای A مورد نظر را بصورت Cname یا Alias، در آن ایجاد می کنیم.
- DNS Server Cache را یکبار پاک می کنیم.
- Client DNS را یکبار پاک می کنیم.
- در PowerShell به ترتیب درج می کنیم:

```
Set-DnsServerGlobalNameZone -AlwaysQueryServer $true
Set-DnsServerGlobalNameZone -Enable $true
Add-DnsServerPrimaryZone -Name GlobalNames -ReplicationScope domain
Add-DnsServerResourceRecordCName -HostNameAlias pc1.payamavar.local -Name C1 -ZoneName GlobalBames
Clear-DnsServerCache
Clear-dnsClientCache
```

یا ipconfig /flushdns

: Recursion policy

یکی از راه های امن کردن **DNS Server** این است که فقط به بعضی **Interface** ها مجوز ارسال و دریافت دستورات **DNS** را بدهیم.
بطور پیشفرض، قابلیت دریافت درخواست های **Recursion** بر روی همه ی **DNS Server** ها فعال است.پس بعضی **Server** هایی که قابلیت **Recursion** روی آنها فعال است، ممکن است درخواست هایی از **IP** های جعلی دریافت نمایند!
با افزایش این درخواستها، ترافیک بالایی برروی **Server** مسیردهی می شود که باعث کند شدن شبکه می شود! پس مدیران شبکه، یا باید **IP** های مربوطه را بلاک کنند و یا قابلیت دریافت درخواست های **Recursion** را غیرفعال کنند.
برای این کار باید روی گزینه ی **Server** موردنظر کلیک راست کرده و وارد **Properties** و تب **Advanced** شد و گزینه ی **Disable recursion** را فعال کرد.
در این حالت، دستور **nslookup** برای مقاصدی که در اینترنت یا شبکه های خارجی هستند، از کار می افتد!

اما یک سیاست در **DNS Server** وجود دارد، به نام **Recursion policy** که توسط آن می توانیم قابلیت **Recursion** را فقط برای بعضی **DNS Server** ها (**Forward Loookup Zone** ها) فعال کنیم.
یک بازه یا **Scope** تعریف کنیم و سپس یک سیاست برای آن تعریف می کنیم، و فقط درخواستهایی که به آدرس **DNS Server** مجاز موردنظر وارد می شوند را در آن **Scope** قرار داده و اجازه ی **Recursion** را فعال می کنیم.
نکته: وقتی گزینه ی **Disable recursion** فعال باشد، ارتباط با اینترنت هم برقرار نمی شود و همچنین در تب **monitoring**، تست **recursive** هم عمل نمی کند!

- یک **Scope** با یک نام دلخواه ایجاد می کنیم که درخواست های **Recursion** (که از شبکه ی خارجی می آیند)، برای آن فعال باشد.

```
Add-DnsServerRecursionScope -Name "Name1" -EnableRecursion $true
```

- یک **Policy** با یک نام دلخواه تعریف می کنیم که درخواست هایی که به **DNS Server** موردنظر (با آدرس **192.168.139.139**) وارد می شوند را به **Scope** ایجاد شده ارجاع بدهد، تا در آنجا **Recursion** برای آنها فعال تعریف شود.

```
Add-DnsServerQueryResolutionPolicy -Name "Name2" -Action allow -ApplyOnRecursion
-RecursionScope "Name1" -ServerInterfaceIP "EQ,192.168.139.139"
```

به این صورت، هردرخواست دیگری که به هریک از **DNS Server** ها یا **Forward Lookup Zone** های دیگر وارد شود، پذیرفته نشده و دفع می شوند.
برای حذف این **Policy**، می توان از دستور زیر استفاده کرد:

```
Remove-DnsServerQueryResolutionPolicy -name "Name2"
```

مثال:
اگر بخواهیم **Client** های فقط یک **Zone**، قادر به ارتباط با محیط اینترنت باشند، اما تمامی **Client** های دیگر نتوانند:

- یک **Scope** ایجاد کرده و **recursion** را برای آن فعال می کنیم:

```
Add-DNSServerRecursionScope -Name 'Scope1' -EnableRecursion $true
```

- قابلیت **Recursion** را برای همه ی **Client** های دیگر غیرفعال می کنیم:

```
Set-DNSServerRecursionScope -Name . -EnableRecursion $false
```

- یک **Policy** ایجاد می کنیم و درون آن، **Scope** ای که ساختیم را به شبکه ی **IP** موردنظر اختصاص می دهیم:

```
Add-DNSServerQueryResolutionPolicy -Name 'Policy1' -Action Allow -ApplyOnRecursion -
RecursionScope 'Scope1' -ServerInterfaceIP 'EQ,10.0.0.100'
```

مثال:

می خواهیم امکان ارسال درخواستها به صورت Recursion، فقط برای کاربران موجود در یک دامین دیگر مثل pa.com با آدرس 10.1.2.244 وجود داشته باشد، اما این Server نباید امکان دریافت درخواستهای Recursion که دارای منبع اینترنتی هستند، را داشته باشد. برای پیکربندی این تنظیم، در DNS Server مورد نظر، وارد PowerShell می شویم:

- ابتدا فناوری Recursion را بطور کل برای دسترسی های خارجی، غیرفعال می کنیم.

```
Set-DnsServerRecursionScope -Name .-EnableRecursion $false
```

- محدوده یا Scope ای ایجاد می کنیم و فناوری Recursion را برای آن فعال می کنیم.

```
Add-DnsServerRecursionScope -Name "Inter-Clients" -EnableRecursion $True
```

- یک Policy با یک نام دلخواه تعریف می کنیم که درخواست هایی که به DNS Server موردنظر (با آدرس 10.1.2.244) وارد می شوند را به Scope ایجاد شده ارجاع بدهد، تا در آنجا Recursion برای آنها فعال تعریف شود.

```
Add-DnsServerQueryResolutionPolicy -Name "Rec-Policy" -Action ALLOW
-ApplyOnRecursion -RecursionScope " Inter-Clients" -ServerInterfaceIP "EQ,10.1.2.244"
```

DNSSEC :

یک راهکار امنیتی برای جلوگیری از حملات DNS Spoofing (جعل DNS) و همچنین DNS Poisoning (مسموم کردن DNS)، این است که توسط قابلیت DNSSEC، DNSServer را Sign یا امضا کنیم.

تا قبل از ویندوز سرور 2012 ارتباطات DNS احراز هویت نمی شدند، پس ارتباط بین Client ها و Server های DNS، غیرامن بود و یک هکر با spoof کردن ترافیک DNS یا نفوذ به داخل local DNS Cache ، می توانست کاربران و برنامه ها را به سمت Site ها و سرویس های مخرب هدایت کند.

از ویندوز سرور 2012 به بعد، DNS server ها توسط DNSSec ملزم شدند که تمام فعل و انفعالات را validate کنند.

توسط DNSSEC کاربران مطمئن می شوند که سایتی که در حال اتصال به آن هستند، دقیقا همان سایت مدنظر خودشان است.
در حقیقت تا حد خیلی زیادی پروتکل SSL هم این اطمینان را بوجود می آورد، اما اگر در جواب یکی از query های DNS، یک IP address جعلی برگردد، دیگر از SSL هم کاری ساخته نیست. به همین جهت DNSSEC اهمیت بالایی دارد.

شیوه ی کار DNSSEC به این صورت است که:
ما نیاز به رمزنگاری اطلاعات داریم که به این جهت از دو Private Key و Public Key استفاده می کنیم.
Private Key فقط در اختیار DNS Server باقی می ماند.
Public Key باید به همه ی Client ها ارسال شود و پیش آنها بماند.
ارسال Public Key به Client ها، توسط Trust Point ها و Trust Anchor ها انجام می شود.
اما، به جهت اینکه نفوذگرها می توانند توسط Trust Point ها وTrust Anchor های جعلی خودشان، یک Public Key دیگر به Client های ما ارسال کنند، ما از یک جدول به نام NRPT (Name Resolution Policy Table) استفاده می کنیم، که این جدول Client ها را مجبور می کند که Public Key را فقط از Trust Point های شبکه ی داخلی دریافت کنند.

راه اندازی DNSSEC :

برای اینکه این تکنیک را بر روی تمام شبکه راه اندازی کنیم، در main DC:

- بر روی Forward Zone مربوط به main DC کلیک راست کرده و DNSSEC و سپس Sign the Zone را می زنیم.
- بطور معمول Use Default Setting را زده و تا پایان پیش می رویم.
- می توانیم روی آن Zone دوباره کلیک راست کرده و DNSSEC را زده و وارد Properties شده و در تب Trust Anchor گزینه ی آنرا Enable کنیم.

دقیقاً همین کار را برای Reverse Zone آن نیز انجام می دهیم.

نکته: اگر پوشه ی Trust Points فعال نباشد، باید در PowerShell دستور زیر را وارد کنیم:

```
dnscmd نام سیستمDNS Server  /config /enablednssec 1
```

برای مشاهده ی فعال بودنِ آن، و یا مشاهده ی لیست Trust Point ها، درج می کنیم:

```
Get-DnsServerTrustPoint
```

حال باید Client ها را مجبور کنیم که این Signing Key های Public را دریافت کنند.

پس وارد کنسول Group Policy Management می شویم، و اگر بخواهیم این اجبار، برای همه ی اعضای شبکه باشد، پس وارد تنظیمات Default Domain Policy شده و به مسیر زیر می رویم:

Computer Configuration > Policies > Windows Setting > Name Resolution Policy >

- در کادر سمت راست، و در نوار Suffix، نام Root DC را درج می کنیم: payamavar.local
- دو گزینه ی Enable DNSSEC و Require DNS clients را فعال می کنیم.
- Create را زده و Apply کرده و Group Policy را از طریق cmd یکبار Update می کنیم.
- برای اطمینان از فعال بودنِ آن در cmd درج می کنیم: **netsh namespace show policy**
- برای اطمینان از امنیتِ Root DC توسط قابلیت Signing، درج می کنیم: **Get-DnsServerZone**

Socket Pool :

می توان DNS Server را طوری پیکربندی کرد که وقتی DNS Query دریافت می کند، بصورت random از اعداد Source Port های مختلف استفاده کند.

این source port ها را درون مخزنی به نام Socket Pool قرار می دهد.

این قابلیت سطح امنیت را بالا می برد، چون وقتی شخصی قصد نفوذ به شبکه از طریق سرویس DNS را داشته باشد، نمی تواند بداند که DNS Server جهت پذیرش Query ها از کدام پورت استفاده می کند.

اندازه ی پیشفرض Socket Pool ها، مقدار 2500 است؛ که می توان آنرا توسط دستور زیر در PowerShell مشاهده کرد:

dnscmd /info socketpoolsize

می توان با دستور زیر، مقداری بین صفر تا ده هزار را برایش تعیین کرد:

dnscmd /config /socketpoolsize عددی دلخواه

نکته: هرقدر این عدد بیشتر باشد، امنیت سرویس DNS بیشتر خواهد بود.

: Cache Locking

وقتی یک **DNS Server** در **Cache** خود، مشخصات یک مقصد را (مثل **Google.com**) در خود ذخیره می کند، دارای یک **TTL** است که یک زمان را مشخص می کند، و تا پایان این زمان، نمی توان محتویات **DNS Cache** را برای این مقصد، **Update** کرد؛ که به این حالت **Cache locking** گفته می شود.

- برای مشاهده ی میزان **Cache Locking** می توان در **PowerShell** درج کرد:

```
Get-DnsServerCache
```

همانطور که می بینیم، مقدار پیشفرض **Locking Percent** بر روی آخرین درجه، یعنی **100** است، که اگر این عدد را کمتر کنیم، میزان **TTL** نیز کاهش پیدا می کند.

- برای تغییر **TTL** میزان **Cache Locking** در **PowerShell** درج می کنیم:

```
Set-DnsServerCache -LockingPercent 90
```

- برای دیدن اطلاعاتی شامل تعداد **IP** ها و میزان **TTL** یک **UNC**، درج می کنیم:

```
Resolve-DnsName payamavar.local
```

:Response Rate Limiting (RRL)

در حقیقت برای جلوگیری از **overload** شدن **Server** توسط فعالیت های **DNS Server**، و یا در برابر حملات هکری مثل **DDOS** یا .... می توان یک سری محدودیت ها برای آن تعریف کرد، که بطور پیشفرض، این محدودیت ها غیرفعال هستند.

برای مشاهده ی آنها درج می کنیم:

```
Get-DnsServerResponseRateLimiting
```

در پاسخ، محدودیت های سرویس **dns** را می بینیم، مثلاً:

- تعداد **Response** هایی که در ثانیه بتواند پاسخ دهد،
- تعداد **Error** هایی که در ثانیه بتواند بررسی کند،
- تعداد **Session** هایی که در ثانیه بتواند برقرار کند،
- حداکثر میزان **Subnetting** برای **IP** های **V4** و **V6** را می بینیم.
- اما مورد **Leakrate** به این معنی است که اگر میزان درخواست های وارده به **DNS** از میزان **Response per secound** بیشتر شد، تا چه میزان را استثنا قائل شده و پاسخ دهد.

- مورد **Mode** شامل سه حالت است:
  - **Enable** : این محدودیتها را اعمال می کند.
  - **Disable** : این محدودیت ها را اعمال نمی کند.
  - **LogOnly** : بدون اعمال این محدودیت ها، فقط میزان **Rate** آنها را گزارش گیری می کند.

برای تعریف یا تغییر این **Rate** ها، بطور مثال، به صورت زیر درج می کنیم:

```
Set-DnsServerResponseRateLimiting -ResponsesPerSec 10 -ErrorsPerSec 10 -WindowInSec 10 -
LeakRate 4 -Mode LogOnly
```

برای بازگرداندن به حالت **Default** :

```
Set-DnsServerResponseRateLimiting -ResetToDefault
```

پس از بازگرداندن به **Default**، می بینیم که **Mode**، هنوز تغییری نکرده! چون **mode** را باید دوباره بصورت دستوری و دستی تغییر داد.

هنگامی که RRL را روشن می کنید، توانایی پیکربندی exception (استثنا) ها را نیز دارید، که می توانید آن را بر اساس اینترفیس های شبکه یا subnet انجام دهید.
به این صورت که اگر DNS server هم به شبکه ی خارجی و هم به داخلی پاسخ می دهد، می توان برای آن تعیین کرد که دریافت ترافیک های داخلی چه حجم بالا داشته باشند چه نه، بدون مشکل هستند.اما اگر ترافیک شدیدی از طریق اینترنت می آید، باید پالیسی های RRL را فعال کنیم.

در اینجا یک Subnet پیکربندی می کنیم تا از RRL مستثنی شود.
نام این Subnet را My Network گذاشته و آن را بر اساس اینترفیس متصل به Server پیکربندی می کنیم، مثلاً می گوییم هر Query که از اینترفیس متصل به سرور 192.168.0.20 می آید، از اعمال شدن RRL استثنا شود.

```
Add-DnsServerResponseRateLimitingExceptionlist -Name “My Network” -ServerInterfaceIP
“EQ,192.168.0.20”
```

اگر دستور زیر را بزنیم، می بینیم که اگر Query هایی از 192.168.0.20 بیایند، با نام My Network شناخته می شوند.

```
Get-DnsServerResponseRateLimitingExceptionlist
```

:DNS Policy

در حقیقت به جهت دسته بندی و پاسخ دادن های مدیریت شده به DNS Query های دریافتی در DNS Server، سیاست هایی را استفاده می کنیم، که این سیاست ها می توانند به شکل های مختلف اعمال شوند، که شامل موارد زیر هستند:

- **Client Subnet** : Subnet هایی تعریف می‌کنیم، به آنها اسم اختصاص داده و بر مبنای آن اسم ها، به درخواست‌ها پاسخ می دهیم.
- **Transport Protocol** : بر مبنای اینکه از پروتکل TCP یا UDP استفاده شده است، به درخواست‌ها پاسخ می‌دهیم.
- **IP** : بر مبنای اینکه از IPv4 یا IPv6 استفاده شده است، به درخواست‌ها پاسخ می‌دهیم.
- **Server Interface IP address** : بر مبنای IP مربوط به NIC که روی Server، درخواست را دریافت کرده است، پاسخ می‌دهیم.
- **FQDN** : بر مبنای FQDN ای که درخواست resolution برای آن ارسال شده است، پاسخ می‌دهیم.
- **Query Type** : بر مبنای اینکه، درخواست از چه نوعی از رکوردها است، پاسخ می دهیم.مثلاً A record ، SRV record و ....
- **Time Of day** : بر مبنای اینکه چه ساعتی از روز، درخواست دریافت شده است، پاسخ می دهیم.

DNS Policy ها بر اساس Level، به دو دسته تقسیم می شوند:

- Server Base: Policy هایی که بر روی Server ها تنظیم می کنیم.
- Zone Base: Policy هایی که فقط بر روی یک Zone تنظیم می کنیم.
  که در این صورت، باید Scope هایی را بر روی Zone موردنظر ایجاد کنیم.

نکته: همیشه اولویت اجرای Policy ها، با Server Base هاست.
اما در صورتی که در سطح Server، چندین policy داشته باشیم، اولویت بندی این Policy ها به وسیله ی عددی به نام ProcessingOrder که برای هریک از Policy ها، تعیین می کنیم و قابل تغییر نیز می باشد، انجام می شود.

برای ایجاد Zone Base DNS Policy ها، ابتدا باید یک Zone ایجاد کرده باشیم، و سپس:

1. Zone Scope تعیین می کنیم:

```
Add-DnsServerZoneScope -ZoneName memser.payamavar.local -Name "h1"
Add-DnsServerZoneScope -ZoneName memser.payamavar.local -Name "h2"
```

برای مشاهده ی Zone Scope ها:

```
Get-DnsServerZoneScope -ZoneName memser.payamavar.local
```

2. فرض کنید که در Zone ای به نام memser.payamavar.local، یک رکورد به نام PC1 داریم و می خواهیم به این رکورد، Zone Scope اختصاص دهیم:

```
Add-DnsServerResourceRecord -ZoneName memser.payamavar.local -A -Name "PC1" -IPv4Address
"192.168.139.166" -ZoneScope "h1"
```

به همین شکل، رکورد PC1 را به یک IP دیگر تحت Zone Scope به نام h2 اختصاص می دهیم.

```
Add-DnsServerResourceRecord -ZoneName memser.payamavar.local -A -Name "PC1" -IPv4Address
"192.168.139.167" -ZoneScope "h2"
```

به همین شکل، رکورد PC1 را به یک IP دیگر برای حالت پیشفرض و بدون Zone Scope اختصاص می دهیم.

```
Add-DnsServerResourceRecord -ZoneName memser.payamavar.local -A -Name "PC1" -IPv4Address
"192.168.139.168"
```

برای مشاهده ی اینکه چه Policy ای بر روی یک Zone تعیین شده است، دستور زیر را وارد می کنیم، که اگر Policy ای تعریف نشده باشد، پاسخی هم نمی دهد:

```
Get-DnsServerQueryResolutionPolicy -ZoneName payamavar.local
```

حال می توانیم سیاست های مورد نظر را تعیین کنیم.

برای اعمال DNS Policy ها از دستور Action استفاده می شود که سه حالت دارد:

- **Allow** : به درخواست، پاسخ مثبت می دهد.
- **Deny** : به درخواست، پاسخ منفی می دهد.
- **Ignore** : به درخواست، هیچ پاسخی نمی دهد و آنرا نادیده می گیرد.

برای حذف یک DNS Policy درج می کنیم:

```
Remove-DnsServerQueryResolutionPolicy -Name نام پالیسی  -Force -ZoneName payamavar.local
```

: Query resolution Policy

3. یک Policy به نام N1 تعریف می کنیم.

- آن را به همه ی رکوردهایی که در همه ی Zone Scope های یک Zone، وجود دارند، اختصاص می دهیم.
- برای هر Zone Scope یک وزن یا اولویت، اختصاص می دهیم.

```
Add-DnsServerQueryResolutionPolicy -Name N1 -Action ALLOW -Fqdn "EQ,*"
-ZoneScope "memser.payamavar.local,1;h1,1;h2,9" -ZoneName "memser.payamavar.local"
```

نکته: -Fqdn "EQ,*" به معنی این است: هر رکوردی (هر FQDN ای)

نکته: برای درج Zone Scope، ابتدا Zone name را درج کرده و با درج یک کاما، وزن و نام Zone Scope را درج می کنیم، و میان آنها یک Semicolon درج می کنیم. و در پایان برای تعیین وزن حالت default (بدون Zone Scope) تنها یک عدد برای وزن آن، درج می کنیم.

برطبق این سیاست:

هربار که درخواست دسترسی به PC1 دریافت می شود، توسط یکی از Zone Scope ها اتصال برقرار می شود. مثلاً:

- در اولین بار که به PC1 درخواستی فرستاده می شود، با Default IP یعنی 192.168.139.168 پاسخ داده می شود.
- و در دومین و سوین بار، با IP مربوط به یکی دیگر از Zone Scope ها پاسخ داده می شود. و ... .

نکته: این درخواست ها را می توان با دستور **nslookup** هم بررسی کرد.

Client Subnet Policy :

3. دو subnet به نام های N1 و N2 با محدوده های زیر، تعریف می کنیم:

```
Add-DnsServerClientSubnet -Name N1 -IPv4Subnet 192.168.139.64/26

Add-DnsServerClientSubnet -Name N2 -IPv4Subnet 192.168.139.128/26

Add-DnsServerQueryResolutionPolicy -Name "26" -Action ALLOW -ClientSubnet "eq,N1" -ZoneScope
"h1" -ZoneName payamavar.local
```

Time of Day :

برای تعریف یک **Policy** به نام **t1** برای جلوگیری از دسترسی به **Zone** ای به نام **payamavar.local** در ساعات غیر اداری:

```
Add-DnsServerQueryResolutionPolicy -Name t1 -Action DENY -TimeOfDay "eq,16:00-08:00"
-ProcessingOrder 1 -ZoneName payamavar.local
```

Logging and Monitoring :

اگر بر روی نام یکی از Server ها در کنسول DNS Server کلیک راست کرده و وارد Properties شوید، به کمک سه تب زیر، می توانید گزارش عملیات DNS را با جزئیات متفاوت بررسی کنید:

- Debug Logging
- Event Logging
- Monitoring

مثلاً در تب Debug Logging می توان قابلیت بسته های Logging را فعال کرده و در نوار پایین، آدرسی برای ذخیره ی فایل گزارش از گزینه های مشخص شده، درج کرد.
این فایل مدام در حال refresh شدن خواهد بود.

برای گزارش گیری از همه ی رکوردهای Zone ، در PowerShell درج می کنیم:

```
Get-DnsServerDiagnostics
```

یکی دیگر از راه های بررسی گزارش گیری های DNS، کنسول Event Viewer است:

- در کادر سمت چپ این کنسول، وارد پوشه ی Applications and Services Logs شده و DNS Server را انتخاب می کنیم و یا وارد پوشه ی Microsoft و Windows و سپس DNS Server می شویم.
- همچنین می توان بر روی گزینه ی DNS Server درون Applications and Services Logs کلیک راست کرده و View و سپس Analytic and Debug Logs را زد، که آنگاه فایلی به نام Analytical درون پوشه ی DNS Server پایین، پدید می آید که شروع به گزارش گیری می کند.

Aging and Scavenging :

این مکانیزم، برای حذف رکوردهای قدیمی استفاده می شود.
معمولاً اگر رکوردهای یک Zone، فعال هم نباشند، در داخل Zone باقی می مانند، که به این رکوردهایی که غیرفعال مانده اند، Stale record گفته می شود.
یک مدیر شبکه باید تصمیم بگیرد که برای یک Stale Record چه اتفاقی رخ دهد.
قابلیت های aging و scavenging ، بصورت پیشفرض غیرفعال هستند.
برای دسترسی به آن، روی Zone موردنظر کلیک راست کرده و وارد Properties و تب General می شویم.
با دو پارامتر زمانی جهت تصمیم گیری مواجه می شویم:

- No Refresh Interval : محدوده ی زمانی ای که طی آن، یک رکورد update نشود، و پس از پایان آن، رکورد Stale می شود.
- Refresh interval : محدوده ی زمانی ست که پس از Stale شدن شروع می شود. در حقیقت مهلتی ست جهت update شدن آن Record.

در این Zone، اگر یک Record پس از گذشت مقدار no-refresh و سپس refresh interval، بطور خودکار به روز نشود، حذف خواهد شد.

برای زمانی است که یک رکورد DNS، به همراه یک برچسب زمانی به DNS zone اضافه می شود.
بخش aging که مثل یک برچسب زمانی ست بر روی رکوردها، به منظور اینکه بتوان این رکورد را پس از مدتی حذف کرد.
مشابه یک بمب ساعتی!
هنگامی که یک رکورد، تغییر کرده یا refresh می شود، این برچسب زمانی Reset می شود.
این قابلیت را از طریق PowerShell نیز می توان کنترل کرد:

```
Set-DnsServerZoneAging payamavar.local -Aging $True -ScavengeServers 192.168.139.123
```

می توان این قابلیت را روی کل DNS پیاده سازی کرد تا روی همه ی Zone ها اعمال شود.
کافیست روی نام DNS Server راست کلیک کرده و وارد Properties شده و در تب advanced و در پایین صفحه، با تیک زدن enable automatic scavenging و مشخص کردن زمان لازم، مقدار refresh را مشخص کنیم که بصورت خودکار، بعد از گذشت زمان مشخص شده، رکوردهای stale شده حذف می شوند.

DANE :

(DNS-Based Authentication of Name Entities)
این فناوری با پروتکل TLSA (Transport Layer Security Authentication) کار می کند و می تواند برای جلوگیری از حملات میانِ شبکه ای یا man-in-the-middle (MiTM) کمک کند، که حمله‌کننده خود را به جای CA معرفی می‌کند و یک گواهی جعلی به کاربر ارسال کرده و کاربر را به Website خود هدایت می‌کند.

با استفاده از Dane می‌توان کاربران را آگاه کرد که باید از کدام Certificate Authority انتظار دریافت Certificate را داشته باشند.

دو کارکرد اصلی DANE :

- مشخص می کند که کدام CA موظف و مجاز به صدور Certificate برای یک Resource می باشد.
- TLS Client ها و هویت Server را بدون یک CA احراز هویت می کند.

DNS Statistics :

برای مشاهده ی آمار و ارقام کامل یک DNS Server:

```
Get-DnsServerStatistics
```

برای مشاهده ی کامل آمار و ارقام یک Zone در DNS Server:

```
Get-DnsServerStatistics -ZoneName payamavar.local
```

برای حذف آمارهای ذخیره شده ی DNS هم می توان دقیقا از دستورات بالا استفاده کرد، فقط به جای Get از Clear استفاده کرد.

: Access to DNS Server

ما می توانیم تعیین کنیم که چه User هایی به DNS Server دسترسی و چه نوع دسترسی ای داشته باشند.
همچنین می توانیم برای هریک از Zone ها هم نوع و میزان دسترسی را مشخص کنیم.
فقط باید روی آنها کلیک راست کرده و Properties را زده و در تب Security آنها را مشخص کرد.
در بخش Users and Groups هم سه گروه هستند که قادر به مدیریت و کنترل DNS Server بطور کامل هستند:

- Domain Admins
- Enterprise Admins
- DNS Admins

: DNS in Group Policy Management

یکی از مهم ترین بخش های DNS، پوشه ی tcp_ است که در زیرمجموعه ی پوشه ی Domain قرار دارد.
درون پوشه ی tcp_ فایلهای تنظیمات اساسی DNS قرار دارند که توصیه می شود این تنظیمات را از اینجا تغییر ندهیم.

برای ایجاد تغییر در تنظیمات DNS می توان از طریق کنسول Group Policy Management ها اقدام کرد.
بر روی گزینه ی Default Domain Controllers Policy کلیک راست کرده و Edit را می زنیم.

برای تنظیمات Policy های مربوط به DNS که به آن DNS Service Records گفته می شود، به مسیر زیر می رویم:
Computer Configuration > Policies > Administrative Templates > System > Net Logon > DC Locator DNS Records

پیشنیاز:
می دانیم که Client های یک شبکه برای اینکه بتوانند از منابع Active Directory استفاده کنند، ابتدا باید توسط Domain Controller ، Authenticate شوند، اما این فرآیند Authentication برای سیستم Client باید سریعتر و بهینه تر صورت بگیرد.
پس فرآیندی که Client یا بعبارتی یک سرویس نصب شده روی سیستم Client طی می کند تا با نزدیک ترین Domain Controller موجود در AD ارتباط برقرار کند، DC Locator نامیده می شود.

DC Locator الگوریتمی است که در پس زمینه ی سرویس Net Logon در سیستم Client کار می کند و ارتباط مستقیمی با پیکربندی های انجام شده در DNS resolution و AD Sites and Subnets برای شناسایی نزدیک ترین DC دارد.
DC Locator ترافیک غیر ضروری شبکه در بین Site ها را با شناسایی و پیدا کردن نزدیک ترین DC، کاهش می دهد.

- **Try next closest Site :** با فعال سازیِ آن، در شبکه هایی با چندین Site، به محض درخواست یک Client، الگوریتم DC Locator تلاش می کند که نزدیکترین Site خلوت و موجود را پیدا کند تا درخواست به او ارسال شود.

TTL یا Time To Live :
هنگامی که شما مثلاً نام دامنه‌ای را در نوار آدرس مرورگر خود وارد می‌کنید، توسط سرویس DNS ، نام دامنه ی شما به IP برمی‌گردد و این آدرس IP و دامنه، در Cache سیستم شما ذخیره خواهند شد تا در دفعات بعد نیاز به درخواست به سمت DNS نباشد و سرعت افزایش یابد.
TTL در DNS به مقدار زمانی گفته می شود که آن آدرس IP و دامنه در سیستم شما Cache می‌شوند.

- **Set TTL in the DC Locator DNS Records :** با فعال سازیِ آن، می توان بر حسب ثانیه مشخص کرد که مشخصات یک IP، چه مدت در سیستم ذخیره شوند.مثلاً مقدار 86400 ، به معنای یک روز خواهد بود.

DNS Implementation in DMZ :

بطورمعمول همه ی اطلاعات مربوط به داخل سازمان که در سروری در بخش DMZ سازمان ها قرار دارند، از نوع فقط خواندنی هستند، تا کسی نتواند آنها را تغییر دهد.

در مورد DNS هم به همین شکل است، به این صورت که همه ی Zone هایی که در DMZ Server وجود دارند، باید از نوع Secondary باشند.

پس Zone های مربوطه در DNS Server شبکه ی داخلی، نباید AD integrated باشند، تا در ادامه درون DNS Server موجود در DMZ، به سادگی یک Secondary Zone از آن Zone، ایجاد کنیم.

و اگر بخواهیم Zone Type را برای یک Zone تغییر دهیم، هم می توانیم وارد Properties آن شده و در تب General اقدام کنیم و هم در cmd یکی از دو دستور زیر را وارد کنیم:

- **برای Zone های Primary :**

```
dnscmd <ServerName> /ZoneResetType <ZoneName> /DsPrimary
dnscmd ifm.payamavar.local /ZoneResetType payamavar.local /DsPrimary
```

- **برای Zone های Stub :**

```
dnscmd <ServerName> /ZoneResetType <ZoneName> /DsStub
```

سپس در DNS Server اصلی شبکه، وارد Properties مربوط به Zone موردنظر شده و در تب Zone Transfer، آدرس DMZ Server را وارد کرده و در پایین همان تب Zone Transfer بر روی Notify کلیک کرده و دوباره آدرس DMZ Server را وارد می کنیم.

IP Version 6 :

در روز سوم فوریه سال 2011 تعدادی از بزرگترین نهادها و گروه ها طی جلسه ای اعلام کردند که تمام آدرس های IP Version 4 اختصاص داده شده اند. پس به کمک همه ی شرکت های بزرگ دیگر تلاش شد تا IP ورژن 6 را بسط و توسعه دهند.

از مهمترین تغییرات در IP، افزایش طول آن از ۳۲ بیت به ۱۲۸ بیت می باشد.

IPv6 نسبت به ورژن 4 دارای امنیت بالاتری است، چون:

- به خوبی از پروتکل IPsec پشتیبانی می کند.
- قابلیت Broadcast را پشتیبانی نمی کند.

.1

IPv4 شامل چهار بخش decimal است، که به هریک از آنها، Octet گفته می شود.
هر Octet می تواند یک، دو و یا سه رقمی باشد.هر Octet توسط یک (.) از بخش دیگر جدا می شود.
IPv6 شامل هشت بخش 4 رقمی ست که در مبنای Hexadecimal بوده و هر بخش توسط کاراکتر Colon یا (:) از بخش دیگر جدا می شود.
به هریک از این بخش ها Quartet گفته می شود.
پس محدوده ی هر Quartet از 0000 تا FFFF می تواند باشد.

0000:0000:0000:0000:0000:0000:0000:0000

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

.2

هر Octet هشت بیت حجم دارد.پس یک IPv4، یک آدرس 32 بیتی است.
هر Quartet شانزده بیت حجم دارد.پس یک IPv6، یک آدرس 128 بیتی است.

توسط IPv4 می توان 2^{32} عدد آدرس IP ایجاد کرد؛ حدود 4 میلیارد!
توسط IPv6 می توان 2^{128} عدد آدرس IP ایجاد کرد؛ حدود ...

.3

برای اینکه دو آدرس IPv6 در یک شبکه باشند، باید حداقل چهار Octet اول آنها یکسان باشند.

.4

روش های ساده سازی و فشرده سازی IPv6 :

- می توان قسمتهایی از آن را که تماماً صفر است، فقط با یک صفر نمایش داد. مثال:

FF05:0000:0000:0000:0000:0000:0000:0002
FF05:0:0:0:0:0:0:0002

- اگر دو بخش و یا بخش های بیشتر، بصورت کاملاً صفر، پشت سر هم بیایند، می توان آنها را با درج فقط :: مشخص کرد.(Compression)

9002:E051:0000:0000:0000:C91D:2601
9002:E051::C91D:2601

- در اعدادی که قبل از آنها صفر می آید، می توان صفر قبل از عدد را ننوشت.

2001:ABCD:0:0198:0:0002:ABCD:0001
2001:ABCD:0:198:0:2:ABCD:1

مثال:

FF05:0000:0000:0000:0000:0000:0000:0002 > FF05::2
F925:00C4 > F925:C4
2001:0000:0000:0000:0000:0000:0000:0001 > 2001::1

در هر IP، فقط یکبار می توان از Compression یا همان :: استفاده کرد:

FF05:0000:0000:0000:0300:0000:0000:0002 > FF05::300:0:0:2 ویا FF05:0:0:0:300::2

نکات:

- IP نمی تواند با :: شروع شود.
- فشرده سازی صفرها با کاراکتر :: فقط یک بار در طول آدرس IP می تواند انجام شود.
- عبارتهای به فرم Hexadecimal برای کامپیوتر هیچ مفهومی ندارند، پس IP باید تبدیل به یک عبارت Binary شود.
  - در این تبدیل مقادیر هر بخش به یک عبارت باینری 16 بیتی تبدیل می شوند.
  - بطور مثال، مدل باینری عدد E051 به صورت مقابل است: 1110 0000 0101 0001
  - یعنی تبدیل شده ی باینری آدرس F0A0:9002:E051:0000:0000:0000:C91D:2601 ، کد زیر است:

1111 0000 10100 0000:1001 0000 0000 0010:1110 0000 0101 0001:0000 0000 0000 0000:0000 0000 0000 0000:
0000 0000 0000 0000:1100 1001 0001 1101:0010 0110 0000 0001

5. ::1/128

آدرس Loopback که برای تست NIC استفاده می شود و در IPv4 بصورت 127.0.0.1 است، بصورت زیر می باشد:

0:0:0:0:0:0:0:1 یا ::1

6. ::/128

آدرس Unspecified همانند 0.0.0.0 در IPv4 است که جهت تعریف آدرس هرگونه مبدایی استفاده می شود.

0:0:0:0:0:0:0:0 یا ::

IPv6 Addressing :

- **Global Unicast :**

این آدرسدهی مشابه Public IP برای IPv4 می باشد که در فضای اینترنت قابل Ping و پیگیری شدن است.
درحال حاضر فقط با عدد 2 یا عدد 3 شروع می شوند.
از 2000 شروع شده و با 3FFF به پایان می رسند.

- **Unique Local Addresses (ULAs):**

این آدرسدهی معادل Private IP برای IPv6 می باشد که در فضای اینترنت قابل Ping و پیگیری شدن نیستند.
با عدد F و یا D شروع می شوند.
مثال:

Fc00::/7
Fdf8:f53b::53

- **Multicast :**

این آدرسدهی، نسخه ی Multicast برای IPv6 می باشد.
با عدد FF شروع می شود.
این نوع آدرس همیشه به عنوان آدرس destination استفاده می شود و نه Source.

- **Link Local :**

  - این آدرسدهی هم نسخه ای کاملاً مشابه با APIPA در IPv4، برای IPv6 می باشد.
  - با عدد FE80 شروع می شود.
  - اگر آدرس source یا destination یک بسته، از نوع Link Local باشد، Router آن را مسیریابی نمی کند.
  - از آنجایی که آدرس های Link Local مشابه با Private IP تنها در شبکه ی جاری معتبر و قابل انتقال هستند، و البته از شبکه Router خارج نخواهند شد (چون Router ها آنها را مسیریابی نمی کنند)، به سادگی می توان به آدرس همه ی Interface های یک Router، یک آدرس Link Local مشابه را اختصاص داد.

- **IPv4-mapped :**

در این نوع آدرسدهی، IPv4 مربوطه را تبدیل به یک IPv6 می کنیم.
به این صورت که با ::ffff: شروع شده و در ادامه، IPv4 به آن ضمیمه می شود.
prefix ID آن برابر با 96 خواهد بود.
یعنی 6 اوکتت اول را صفر گرفته و ip mapping تنها در دو اوکتت آخر انجام می شود.
نکته: هر IPv4، در اوکتت آخر، جاسازی خواهد شد.
مثال:

0:0:0:0:0:0:ffff:192.168.0.27
::ffff:192.168.0.27

در DHCP برای IPv4 ، به هر Client چهار ویژگی زیر را اختصاص داده می شود:

- IP Address
- Subnet Address
- Gateway Address
- DNS Server Address

اما DHCP برای IPv6 فقط سه ویژگی زیر را اختصاص می دهد؛ چون دریافت آدرس Gateway یا همان Router، در IPv6 توسط خود پروتکل NDP انجام می شود:

- IP Address
- Subnet Address
- DNS Server Address

: Multicast Addresses

نکته: در سیستم IPv6 هیچ قابلیت Broadcast ای برای ارسال IP ها وجود ندارد!
برای قابلیت Multicast در ورژن 6، می توان یک Packet را:

- فقط برای Client ها ارسال کرد.
- فقط برای همه ی Router ها ارسال کرد.
- فقط برای Router های خاص ارسال کرد.
- و ...

Address	Multicast Group
FF02::1	All Nodes
FF02::2	All Routers
FF02::5	OSPFv3 Routers
FF02::6	OSPFv3 Designated Routers
FF02::9	RIPng Routers
FF02::A	EIGRP Routers
FF02::B	Mobile Agents
FF02::C	DHCP Servers/Relay Agents
FF02::D	All PIM Routers

NDP (Neighbor Discovery Protocol) :

در حقیقت IPv6 تحت پروتکلی مهم به نام NDP کار می کند.

در این پروتکل چهار بسته ی اصلی وجود دارد :

- (NA) Neighbor Advertisement ✓
- (RS) Router Solicitation ✓
- (RA) Router Advertisement ✓
- (NS) Neighbor Solicitation ✓

بیشتر عملیات پروتکل NDP با یک یا چند از بسته های فوق انجام می شود.
هسته ی اصلی این پروتکل، پروتکل ICMP است، اما ورژن 6.(ICMPv6)

برخی کاربردهای پروتکل NDP :

- پیدا کردن Router یا Router Discovery که در مرحله ی Solicit انجام می شود، از بسته های RA و RS استفاده می کند.
- به این صورت که Client ابتدا یک بسته ی RS را بصورت Multicast با آدرس FF02::2 در شبکه ارسال می کند و در پایان Router موردنظر، یک پیام RA را بصورت Unicast برای Client بر می گرداند.

- تشخیص Prefix شبکه، که از بسته های RA و RS استفاده می کند.

- یکسان بودن IP ها را جلوگیری می کند،یا بقولی تشخیصِ یکتا بودن آدرس را توسط پروتکل DAD (Duplicate Address Detection) (تشخیص آدرس تکراری) را انجام می دهد که از بسته های NS و NA استفاده می کند.

- مکانیزم ARP را جهت پیدا کردن آدرس Mac مقصد، پشتیبانی می کند، (Neighbor Mac Discovery) که از بسته های Neighbor Solicitation و Neighbor Advertisement استفاده می کند.

برخلاف IPv4 که پروتکل ARP در آنجا در لایه ی 2 کار می کرد، در IPv6، پروتکل ARP در لایه ی 3 کار می کند.
این قابلیت به این شکل است که ابتدا Client 1 بسته ی NS را به Client 2 ارسال می کند، و با توجه به در اختیار داشتن آدرس IP او، آدرس MAC او را درخواست می کند و Client 2 در صورت صحت مشخصات، توسط یک بسته ی NA، آدرس MAC خودش را به او پس می فرستد.

در IPv6 به دو طریق می توان به Client ها آدرس دهی کرد:

- ○ بصورت دستی
- ○ از طریق DHCP
- ○ از طریق پروتکل SLAAC (Stateless Address Autoconfiguration):
که توسط Router انجام می شود و از بسته های RA و RS استفاده می کند.

: IPv6 Subnetting

در IPv6 آن را به دو نیمه تقسیم می کنند با نام های زیر:

Subnet prefix | Interface suffix

مقدار **Subnet prefix** با مقدار **Interface suffix** همیشه برابر بوده و هریک دارای **64** بیت می باشند.

در **IPv4** مفهومی وجود دارد به نام **Net mask** که محدوده ی **Net ID** و **Host ID** بر اساس آن مشخص می شود که معادلِ آن در **v6** ، با عنوان **Prefix** یا **Subnet ID** و بصورت یک عدد در پایان **IP** درج می شود.
عدد **Prefix** ، مقدارِ ثابت بخش **Subnet prefix** را در سمت چپ **IP** مشخص می کند، که به این مقدار ثابت **Global Routing Prefix** گفته می شود.
اگر **Prefix** برای یک **IP** مشخص نشود، به طور پیش فرض، **64** بیت در نظر گرفته می شود، به همین جهت به **Subnet prefix** معمولاً **Subnet ID** هم گفته می شود!

بطور مثال **IP** مقابل را در نظر بگیرید: **2001::3/32**
در اینجا عدد **32** به این معنی است که **32** بیت از سمت چپ، ثابت و نشاندهنده ی مقدار **Prefix** می باشد.

2001:0:0:0:0:0:0:3 /32

- : **Global Routing Prefix** (2^{32} بیت)
- : **Subnet ID** : انتهای محدوده ی **subnet Prefix** می باشد.
- : **Interface suffix** : تعداد **Client** هایی که می توان در شبکه داشت، معادل **Host ID** در **IPv4** می باشد.(2^{64} بیت)

و این یعنی اینکه می توان 2^{32} شبکه را آدرس دهی کرد، و هریک از این شبکه ها می تواند 2^{64} کلاینت داشته باشد.

:Reverse Zone for IPv6

برای **IPv6** نیز می توان در **DNS Server** هم **Forward** و هم **Reverse Lookup Zone** تعریف کرد.
فقط باید دقت داشت که برای **Reverse Lookup Zone** و درج آدرس آن، باید **Subnet prefix** را همراه با عدد **Subnet** آن، بطورمثال بصورت زیر وارد کرد:

2001:db8:23::/64

DHCP (Dynamic Host Configuration Protocol) :

به فرآیند اختصاص یک IP Address ورژن 4 به یک دستگاه در شبکه، DORA گفته می شود:

- **Discover** : وقتی یک Node به شبکه متصل می شود، برای دریافت IP Address، یک بسته ی Broadcast در شبکه ارسال می کند؛ (به نام DHCP Discover) که جهت پیدا کردن یک DHCP Server است.
به این صورت که مبدا این پیام را با 0.0.0.0 و مقصد آن را با 255.255.255.255 مشخص می کند.اما در حقیقت Mac Address خودش را نیز به این پیام، ضمیمه می کند.

- **Offer** : وقتی که DHCP Server پیام آن Node را دریافت می کند، از IP های آزادی که مجاز به تخصیص آنهاست، یکی را به عنوان جواب آن Node، به او پیشنهاد می دهد.
این پیشنهاد هم در قالب یک پیام Broadcast به مقصد 255.255.255.255 است که البته آدرس MAC ای که دریافت کرده بود و همچنین آدرس MAC خود DHCP Server را نیز ضمیمه می کند.

- **Request** : وقتی که دستگاه موردنظر، Offer را دریافت کرده و حاضر به پذیرشِ آن IP باشد، پیامی به عنوان قبول کردنِ پیشنهاد و درخواست برای تخصیص آن IP به سمت DHCP Server ارسال می کند.

- **Acknowledge** : DHCP Server درخواستِ Node را با یک پیام تأیید به سمت او، می پذیرد.

- وقتی یک کامپیوتر، درخواست ورود به شبکه را می دهد:
  - ابتدا نزدیکترین سیستم DHCP Server، به آن Offer ارسال می کند.
  - پس از اینکه کامپیوتر، IP را دریافت کرد، جهت ذخیره سازی، آن را به DNS Server ارسال می کند تا آن را ثبت کند. (و DNS Server یک A Record برای آن ایجاد خواهد کرد.)
  - همچنین پس از اینکه DHCP Server یک IP به یک دستگاه اختصاص می دهد، نام آن دستگاه را به DNS Server ارسال می کند. (و DNS Server یک PTR Record برای آن ایجاد خواهد کرد.)

- اگر دو Client در شبکه، دارای یک آدرس IP یکسان باشند، IP Conflict ایجاد شده و هر دوی آنها، دسترسی شان به شبکه را از دست می دهند.

DHCP موارد زیر را بصورت خودکار به هر یک از اعضای شبکه اختصاص می دهد :

- ✓ IP Address
- ✓ Subnet Address
- ✓ Gateway Address
- ✓ DNS Server Address

درنتیجه، وقتی که در شبکه، یک DHCP Server وجود دارد، نباید هیچیک از سیستم های عضو شبکه، دارای Static IP باشند، مگر اینکه آدرس Static آن سیستم موردنظر، در DHCP Server، به صورت exclude ثبت شده باشد.

سه نوع اختصاص آدرس های IP در سرویس DHCP وجود دارد:

- Scope : اختصاص یک محدوده ی خاص از IP ها به Client های شبکه.
- Exclusion : مجزا کردن یک یا تعدادی از IP های Scope، جهت جلوگیری از اختصاص آنها در شبکه.
  آدرس های Exclusion، آدرس های Client هایی هستند که Static IP خواهند داشت.
- Reservation : نگه داشتن یک یا تعدادی IP برای یک یا تعدادی از سیستم های موردنظر در شبکه.

نکته: برای انجام reserve IP نیاز به MAC Address سیستم موردنظر خواهیم داشت، که DHCP خودش بطوردقیق آن را اختصاص دهد.

APIPA (Automatic Private IP Addressing) :

زمانی که یک Client، پاسخ مناسبی را از سرویس دهنده ی DHCP دریافت ننماید، یعنی هیچ Offer ای به سوی او ارسال نشود، پس از مدت کوتاهی، یک آدرس تصادفی را در بازه ی 169.254.0.0 تا 169.254.255.255 دریافت می نماید، که این آدرسدهی تصادفی، توسط سرویسی به نام APIPA و از کارت شبکه ی خودش انجام می شود.

آدرس IP خصوصی (APIPA) یک هشدار امنیتی به منظور فقدان DHCP است.

در این حالت، سیستم نه Default Gateway Address دارد و نه DNS Address!

- ✓ Client هایی که از APIPA استفاده می نمایند، در بازه های زمانی پنج دقیقه-پنج دقیقه، شبکه را به منظور وجود یک سرویس دهنده ی DHCP بررسی می نمایند، و اگر سرویس دهنده یDHCP در دسترس قرار بگیرد، سرویس گیرنده، یک درخواست برای وی ارسال، و اطلاعات مربوط به پیکربندی TCP/IP را از آن دریافت می نماید.

Lease Duration :

در حقیقت Lease Duration یک مقدار زمانی است که مدت زمانی را که هر IP اختصاص داده شده، معتبر باقی می ماند، و پس از آن، باید تمدید اعتبار و یا تعویض شود را مشخص می کند.

اما در حقیقت، DHCP Server دقیقاً تا پایان مدت زمان Lease Duration صبر نمی کند، بلکه دو بار آدرس IP و مقدار Lease Duration آن را بررسی می کند:

وقتی که 50٪ از زمان مورد نظر گذشته باشد.مثلاً اگر عدد را بر روی 100 روز گذاشته باشیم، پس از روز 50 اُم، چک می کند.

اگر به هر دلیلی Client برای بررسی اول، در دسترس نباشد، DHCP Server صبر کرده و زمانی که 87.5٪ از زمان Lease Duration گذشته باشد، دوباره سعی به چک و بررسی می کند.

نکته: این عملیات renew، فقط شامل دو مرحله ی پایانیِ فرآیند DORA می باشد، یعنی Request و Acknowledge.

اما اگر در بار دوم هم موفق به تمدید IP Address مربوط به Client نشود، در پایان اعتبار Lease Duration تمام چهار مرحله ی دریافت IP از DHCP Server برای آن Client انجام خواهد شد.

- با هربار Resetart شدن سیستم های Client، این Renewal یا تمدید IP Address برای آنها انجام می شود.
- با هربار disable/Enable کردن آداپتور کارت شبکه، این Renewal یا تمدید IP انجام می شود.

بطور پیشفرض، مقدار Lease Duration :

- در شبکه های Wired برابر است با 8 روز
- در شبکه های Wireless برابر است با 8 ساعت

نکته: اگر Client هایی که به یک Scope متصل می شوند، مدت زمان طولانی ای متصل نخواهند بود، lease duration را کم می کنیم.

نکته: برای اینکه بصورت دستی این عملیات renewal را انجام دهیم، می توانیم در cmd دستور زیر را درج کنیم:

```
Ipconfig /renew
```

اگر Client هایی که به یک Scope متصل می شوند، مدت زمان زیادی را متصل نخواهند بود، باید **lease duration** آن Scope را کوتاه تر تنظیم کنیم.

: Verifying the DHCP Server Connection

در حقیقت برای اینکه بررسی کنیم که آیا Client جاری با DHCP کاملاً در ارتباط است و DHCP به آن سرویس می دهد یا نه، باید در cmd یکبار IP ای که در حال حاضر در اختیار Client است را آزاد کرد، و دوباره درخواست IP به سرور ارسال کرد.
پس دستورهای زیر را یکی یکی و با فاصله ی زمانی چند ثانیه از هم، درج و وارد می کنیم:

Ipconfig /release
Ipconfig /renew

: Installation DHCP Server

- بهترین حالت برای DHCP، این است که یک DHCP Server جدا از AD DS Server راه اندازی شود.
- قبل از راه اندازی DHCP Server، لازم است که IP سیستمش، Static باشد.
- DHCP Server نمی تواند بر روی دستگاه های NANO Server راه اندازی شود.
- در Server manager وارد Add Roles and Features شده و نقش DHCP Server را انتخاب و در بخش Feature، از زیرگزینه های Remote Server Administration Tools، گزینه ی Role Administration Tools و سپس گزینه ی DHCP Server Tools را انتخاب کرده و نصب را تا پایان پیش می رویم.

Install-WindowsFeature DHCP -IncludeAllSubFeature -IncludeManagementTools	نصب تحت PowerShell
Uninstall-WindowsFeature DHCP -IncludeAllSubFeature -IncludeManagementTools	حذف تحت PowerShell
Dism /online /enable-feature /featurename:DHCPServerCore	نصب تحت cmd
Dism /online /disable-feature / featurename:DHCPServerCore	حذف تحت cmd
gcm -Module DHCPServer	دریافت دستورات PowerShell

سپس وارد ویزارد Configuration شده، یک User انتخاب کرده و تا پایان پیش می رویم.
وقتی برای اولین بار وارد کنسول DHCP Manager می شویم، یک بار آن را Reset می کنیم:
روی نام Server در کادر سمت چپ کنسول، کلیک راست کرده و از طریق All Task، گزینه ی Restart را می زنیم.

- اگر DHCP Server بر روی سیستم DC نصب و راه اندازی شود، تمام DHCP Server های دیگر موجود در شبکه را از کار خواهد انداخت و سرویس دهی را تنها خودش انجام می دهد؛ که برای راه اندازی DHCP Server های دیگر، باید آنها را نیز authorize کرد. به صورت زیر:

netsh dhcp add server <ServerDNSDomainName> <ServerIPAddress>
netsh dhcp add server dc1.payamavar.local 192.168.139.144

حال اولین کاری که باید کرد، این است که یک Scope ایجاد کنیم:

- روی IPv4 کلیک راست کرده و New Scope را می زنیم.
- یک Name برای آن تعیین می کنیم.
- رنج IP موردنظر و مقدار Net Mask و Subnet Mast را برای این Scope مشخص می کنیم.
- رنج Exclusion IP ها و یا IP موردنظری که می خواهیم exclude کنیم را وارد و Add می کنیم.
- اگر بیش از یک DHCP Server در شبکه داشته باشیم، لازم است که مقدار **Subnet dely in milli Second** را تعیین کنیم، به این صورت که اگر می خواهیم این DHCP Server برای ارائه ی پیام Offer به Client ای که درخواست IP داشته است، در اولویت تر باشد،

- این مقدار را در کمترین حالت قرار می دهیم، و اگر می خواهیم که **DHCP Server** دیگر در اولویت تر باشد، برای این مقدار، عدد بیشتری را وارد می کنیم.
- حال باید زمان **Lease Duration** را تعیین کنیم.
- آدرس **Default Gateway** که معمولاً مربوط به **Router** است را وارد می کنیم.
- نام **Domain** و مشخصات **DNS Server** را وارد می کنیم.
- تب **Wins Server** را رها می کنیم و تمام!

برای ایجاد یک Scope از طریق PowerShell :

Add-DhcpServerv4Scope -Name SCP1 -StartRange 10.0.1.1 -EndRange 10.0.1.50 -State Active -SubnetMask 255.255.255.0

نکته: به تعداد NIC های سیستم DHCP Server می توان Scope ایجاد کرد.

هر Scope یک Scope Name دارد که در تب اول، برای آن ایجاد کردیم، و یک Scope ID که در حقیقت Net Address مربوط به محدوده ی تعیین شده برای آن، می باشد.(همه ی بیت های Host ID آن صفر هستند.) مثلاً: 192.168.1.0

- **به ازای هر پورت از NIC، مربوط به سیستم ای که DHCP Server روی آن نصب است، می توان یک Scope تعریف کرد.**
- به عبارتی، به ازای هر **Scope** در **DHCP**، باید یک کارت شبکه هم موجود باشد.
- **برای مشاهده ی مشخصات Scope هایی که درون یک DHCP Server وجود دارند، در PowerShell درج می کنیم:**

Get-DhcpServerv4Scope -ComputerName ifm

- **Address Pool : کلیه ی آدرس های IP که برای این Scope تعریف می کنیم، در این قسمت قرار می گیرند.**
- **Address Lease : هر Client ای که به شبکه متصل شده و از DHCP Server یک IP دریافت کند، در این قسمت قرار می گیرد.**

نکته:
کاربرانی که عضو گروه DHCP Users هستند، می توانند در کنسول DHCP سرور، Scope ایجاد کنند.
کاربرانی که عضو گروه IPAM Users هستند، می توانند در IPAM سرور، Scope ایجاد کنند.

General settings of DHCP :

کشف DHCP Server :

برای دریافت لیست DHCP Server های مجاز در شبکه، از یکی از دو دستور زیر استفاده می کنیم:

```
Get-DhcpServerInDC
Netsh DHCP show server
```

تعیین کارت شبکه:

اگر بیش از یک NIC بر روی Server داشته باشیم، می توانیم مشخص کنیم که DHCP عملیات آدرس دهی را بر اساس کدام یک بدهد یا ندهد، پس وارد Properties آبجکت IPv4 می شویم، در تب Advanced بر روی Bindings کلیک می کنیم و آنرا مشخص می کنیم.

پیشگیری از ثبت و سرویس دهی به Client ای با نام مشابه با یک Client که از قبل در DHCP ثبت شده:

- گاهی ممکن است دو Client نامی یکسان داشته باشند، برای جلوگیری از ثبت و Update شدن Client دوم در DHCP، از درون Properties مربوط به Scope، وارد تب DNS شده و گزینه ی Name Protection را Enable می کنیم.

نکته: در حقیقت این مشکل برای سیستم های ویندوزی رخ نمی دهد، بلکه زمانی که سیستم غیرویندوزی وارد شبکه می شود.

رفع ایرادات:

- وقتی کنار آیکون یک Scope، علامت قرمز باشد، یعنی Scope غیرفعال است که باید Active شود!
- وقتی کنار آیکون یک Scope، علامت آبی باشد، به یکی از دلایل زیر است:
  - Scope همه ی IP هایش را اختصاص داده است:
    یا <u>باید آنرا reconfigure کنیم</u> (Set-dhcpServerV4Scope) و یا <u>lease duration آن Scope را کم کنیم</u>.
  - آدرسهایی بصورت Bad_Address وجود دارند که باید حذف شوند.
- می توانیم مشکلات و اختلالات DHCP Server را بطورکلی بررسی کنیم، کافی ست بر روی IPv4 کلیک راست کرده و گزینه ی Reconcile All Scopes را زده و در پنجره ی باز شده، Verify را بزنیم، و اگر ایرادی بود با انتخاب آن، آن را برطرف کنیم.

به روزرسانی:

وارد Properties آبجکت IPv4 شویم:

در تب General، می توانیم با فعال کردن .Automatically Update Statistics every، تعیین کنیم که آمار DHCP را هر چند مدت به روز کند.

آمار:

برای مشاهده ی این Statistics کافی ست بر روی IPv4 کلیک راست کرده و Display Statistics را بزنیم.

با فعال کردن گزینه ی Enable DHCP audit logging می توانیم گزارش هایی از DHCP Server را ذخیره کنیم که این گزارش ها در یک فایل ذخیره می شوند و برای آدرسدهی این فایل، باید به تب Advanced مراجعه کنیم.

جلوگیری از تداخل ها:

برای اینکه DHCP قبل از اختصاص یک IP به یک Client، بطورکلی در شبکه چک کند که آن IP ای که برای ارسال آماده کرده، هنوز اختصاص داده نشده است، می تواند چندبار آن آدرس را در شبکه Ping کند، که اگر جوابی نشنید، یعنی آن IP آزاد است.

برای تعیین این مقدار Ping، وارد Properties مربوط به IPv4 شده و در تب Advanced یک عدد برای Conflict detection attempts درج می کنیم.

این عدد باید بزرگتر از صفر و کوچکتر از 6 باشد.

باید دقت داشت که هرقدر این عدد بزرگتر باشد، سرعت اختصاص یافتن IP به Client ها کمتر خواهد بود.

Reservations :

- بطورکلی هر Client در هر درخواست IP از DHCP Server ، یک Dynamic IP دریافت می کند.
- حال اگر بخواهید برخی از Client ها، در هر بار ورود به شبکه، یک IP ثابت از DHCP Server دریافت کنند، می توانید با استفاده از Reservation آن IP را برای آن Client خاص Reserve کنید که در نتیجه آن Client دارای یک IP Static از سمت DHCP Server خواهد بود.
- IP هایی که در این پوشه قرار می گیرند، بطور اختصاصی، برای Client هایشان، رزرو و ثابت می مانند.
- از این قابلیت، برای اختصاص IP به دستگاه هایی مثل Printer ها و Server ها و مشابه آنها استفاده می شود که نیاز است که آدرس ثابتی داشته باشند.
- برای ایجاد یک Reserve Address کافی ست که روی این پوشه کلیک راست کرده و new Reservation را بزنید.
- نکته: از آنجایی که وارد کردن MAC Address سیستم مقصد اجباری است، به یکی از سه طریق زیر MAC Address سیستم مقصد را پیدا می کنیم:

1. پشت سیستم مقصد نشسته و آن را پیدا می کنیم.
2. در همان سیستم DC از طریق PowerShell به آن یک Session زده و آدرس Mac آنرا پیدا کرد:

enter-PSSession نام کامپیوتر مقصد

getmac و یا ipconfig /all

Exit-PSSession

3. در همان سیستم DC در cmd دستور زیر را وارد می کنیم: **Arp -a**

برای Reserve کردن یا ثابت نگه داشتن IP مربوط به Client هایی که در پوشه ی Address Lease قرار دارند، کافی ست روی آنها کلیک راست کرده و گزینه ی Add to Reservation را بزنیم.

- برای اختصاص دادن یک Reserved IP به یک Client و یا تبدیل کردن یک Leased Address به یک Reserved Address از طریق PowerShell:

Add-DhcpServerv4Reservation -ScopeId 192.168.139.0 -IPAddress Leased Address -ClientId Mac Address

DHCP Option :

تمام تنظیماتی که در پوشه ی Server Options تعریف می شوند، بر روی کلیه ی Scope Option ها بصورت پیشفرض، اعمال شده یا به قولی inheritance می شوند.

بعد از تعریف یک Scope، پوشه ی Scope Option برای آن ایجاد می شود که دربردارنده ی تنظیمات مربوط به آن Scope می باشد.

همیشه اولویت اعمال Option ها، با Option پایین تر است:

1. **اول Option مربوط به خود یک Reserved Address**
2. **سپس Class Option**
3. **و بعد Scope Option**
4. **و در پایان Server Option: تنظیمات این بخش، بر روی همه ی Scope ها و Client های متصل به آنها اعمال می شود.**

نکته: در حقیقت این اولویت بندی ها، در مورد Policy ها هم صدق می کنند.

مثال:

اگر در Scope Option تنظیم شده باشد که Router یا همان Default Gateway را سیستم A قرار بده، اما در Server Option تنظیم شده باشد که Router را سیستم B قرار بده؛ Client های عضو Scope، سیستم A را به عنوان Router خود قرار می دهند!

نکته: اگر تنظیمی در Scope Option اعمال نشده باشد، آن Scope بطورکامل از تنظیمات Server Option تبعیت خواهد کرد.

- **برای ایجاد یک Scope Option کافیست روی پوشه ی آن کلیک راست کرده و Configure Options را بزنیم.**
- **برای ایجاد یک Server Option روی پوشه ی آن کلیک راست کرده و Configure Option را می زنیم؛ یک IP تعریف و Add کرده و OK.**

  حال اگر به Scope Option یا Reservation ها برویم، می بینیم که این Option برای آنها نیز تعریف شده است.
- **به همین شکل هم می توان یک Sope Option ایجاد کرد.**

- **برای حذف یک Server Option فقط در خود پوشه ی Server Option ها؛**

  و برای حذف یک Scope Option، فقط در خود پوشه ی Scope Option مربوط به آن، می توان آن را حذف کرد.

از طریق PowerShell برای ایجاد یک Server Option که مقادیر DNS Server و Default Gateway را تعیین می کند:

```
Set-DhcpServerv4OptionValue -ComputerName NAME -DnsServer 192.168.139.139 -Router 192.168.139.2
```

NAME: **باید FQDN این سیستم را درج کنیم.**

Router: **آدرس Default Gateway را دریافت می کند.**

نکته: وقتی در Scope Option ها تغییراتی را اعمال می کنیم، این تغییرات به Client ها ارسال نمی شود، تا زمانی که Renewal کنند.

DHCP Policy :

ما می توانیم در کنسول DHCP Server سیاست های زیادی تعریف کنیم، که اگر یک Device با یک سری مشخصات خاص، درخواست IP کرد، از چه Range ای و یا کدام IP را و چه نوع سرویسی از DHCP را دریافت کند.

برای ایجاد یک Policy، بر روی پوشه ی Policies (مربوط به Scope)کلیک راست کرده و New Policy را می زنیم.

- پس از تعیین نام، در پنجره ی Conditions، با کلیک بر روی Add می توانیم مشخص کنیم که سیستمی که چه مشخصاتی داشته باشد.
  مثلاً تعیین یک MAC Address ! همانطور که می بینیم می توان شرایط را با هم AND یا OR در نظر گرفت.
- اگر فقط یک Condition تعریف کنیم، آنگاه با زدن Next می توانیم Option های بیشتری را مشخص کنیم.

نکته: DHCP Policy ها، به Client های reserve شده اعمال نمی شوند!

تنظیماتی که می توان توسط DHCP Policy اعمال کرد:

- Router : تعیین Router
- Time Server : تعیین Network Time Server موجود در شبکه
- و ...

مثال: فرض کنید چندین دوربین مدار بسته به شبکه متصل هستند که دارای MAC Address های مشابه هستند و قصد دارید آدرس های IP آنها مشخص کنید.

1. بر روی پوشه ی Policies کلیک راست کرده و New Policy را می زنیم.
   - یک نام درج کرده و سپس در پنجره ی Conditions، بر روی Add کلیک می کنیم.
   - در قسمت Criteria گزینه ی MAC Address و در قسمت Operator گزینه ی Equals و در قسمت Value، سه قسمت اول MAC Address های دوربین ها را درج می کنیم.
   - گزینه ی Append wildcard را فعال می کنیم که ادامه ی آدرس ها را (هرچیزی) * در نظر بگیرد.

   نکته: اگر Prefix wildcard را فعال کنیم، علامت * را در ابتدای آن سه بخش قرار می دهد.
   - Add را می زنیم و OK!
   - در تب بعد می توان یک IP Address Range را تعیین کرد.
   - سپس آدرس های DNS و Rooter را نیز می توان تعیین کرد.

مثال: برای اینکه Client هایی که عضو Domain نیستند اما از DHCP آدرس دریافت می کنند، در یک DNS Zone خاص در DNS Server ذخیره شوند، یک DHCP Policy بر اساس FQDN ایجاد کرده و DNS Properties را برای آن تنظیم می کنیم.

مثال: برای اینکه یک سری Client ها مثلاً دستگاه های Wireless که بخشی از ابتدای Mac Address آنها مشابه است، نام آنها در شبکه، دارای یک پیشوند مختص به خود باشد، از IPv4 باید DHCP Policy Configuration Wizard را تنظیم کنیم.
مثلاً: mobile.payamavar.local

: Class Option

با استفاده از DHCP Class ها می توانیم به بعضی Client های دلخواه، Option هایی جدا از آنچه که در Scope شان دریافت می کنند را به آنها اعمال کنیم. مثلاً می خواهیم بعضی Laptop های یک Scope دارای Lease Time کمتری نسبت به بقیه ی اعضای یک Scope باشند!

دو نوع Class وجود دارد:

1. User Classes : در این دسته، Client ها را به شکل کلی مشخص می کنند، مثلاً : لبتاپ ها؛ یا PC ها؛ یا ....
2. Vendor Classes : در این دسته، Client ها را بر اساس مُدل و سازنده شان مشخص می کنند، مثلاً HP ها، یا سیستم های Linux و ....

ایجاد و راه اندازی و اختصاص یک User Class:

1. ابتدا یک Class ایجاد می کنیم، سپس یک Policy به آن اختصاص می دهیم:
   - بر روی IPv4 کلیک راست کرده و Define User Classes را می زنیم.
   - Add را زده و یک Name برای آن درج می کنیم.
   - در پایین همان کادر New Class، در ستون ASCII، باید یک کلمه ی کوتاه درج کنیم، که Class ID نام دارد و در ادامه به آن نیاز خواهیم داشت.مثلاً می توان همان Name ای که انتخاب کردیم را درج کرد!

2. حال یک Policy ایجاد می کنیم.
   - در تب Configure Conditions گزینه ی Add را زده و در قسمت Criteria گزینه ی User Class را و در قسمت Value گزینه ی Class ای که ایجاد کردیم را انتخاب و Add می کنیم.
   - در تب Configure Setting .. هر تنظیم دلخواهی را تعیین کرده و next.

3. حال باید آن Class ای که ایجاد کرده بودیم را به هر Client دلخواه، نسبت دهیم.
   - پس در هریک از سیستم های Client وارد cmd شده و توسط نام آداپتور NIC، دستور زیر را وارد می کنیم:

```
ipconfig /setclassid "ethernet0" MyClassID
```

   - سپس یکبار NIC را قطع و وصل می کنیم تا تنظیمات اعمال شوند.

نکته:

- هر کارت شبکه (NIC) فقط می تواند یک Class ID را دریافت کند.
- برای اینکه متوجه شویم که آیا Client دارای یک Class ID است یا نه، از دستور ipconfig /all استفاده می کنیم.
- برای خارج کردن یک Client از Class ID ای که دریافت کرده بود، دستور زیر را در cmd درج می کنیم:

```
ipconfig /setclassid "ethernet0"
```

✓ Client ای که Class ID دریافت می کند، نباید جزو کامپیوترهای دارای آدرس Reserve شده باشد، چون MAC Addreess یک Reserved Client در DHCP ثبت شده است و Policy روی آن اعمال نمی شود.

ایجاد و راه اندازی و اختصاص یک Vendor Class، کاملاً مشابه با User Class می باشد.

: DHCP Server Migration

فرض کنید بخواهیم در DHCP Server، فقط یک Scope را کاملاً به یک کامپیوتر دیگر انتقال دهیم.

1. در Server جدید، نقش DHCP Server را نصب می کنیم.

2. از Scope موردنظر در DHCP Server قدیمی یک Export تهیه می کنیم:
در PowerShell دستور زیر را وارد می کنیم:

Export-DhcpServer -Leases -File C:\dhcpFile.xml

پس Export در قالب یک فایل XML به نام dhcpFile و در درایو C ذخیره می شود.

3. سرویس DHCP را بر روی سرور قدیمی، Stop می کنیم:
در کنسول DHCP، بر روی نام کامپیوتر Server کلیک راست و All Task و Stop را می زنیم.

4. در DHCP Server جدید، فایل Export شده را Import می کنیم.
در PowerShell دستور زیر را درج می کنیم:

Import-DhcpServer -Leases -File C:\ddhhccpp.xml -BackupPath c:\Pooshe

در حقیقت از یک آدرس، فایل Export شده را وارد می کنیم، و در آدرس دیگر که برای پارامتر BackupPath تعیین کردیم، یک Backup از آن تهیه می کنیم که در صورت بروز آسیب به فایل Backup، قابل بازیابی باشد.این Backup گیری در حین Import آن، اجباری است!

: Multicast Scope

این Scope جهت تخصیص IP های D Class یعنی بین 224.0.0.0 تا 239.225.255.255 به Client ها در زمانی که قصد شرکت در یک عملیات Streaming (ارسال و دریافت یک رشته از داده های پیوسته مثل Viedo chat) را دارند، استفاده می شود.
زمانی که Client ها بخواهند در چنین عملیاتی شرکت کنند، بجای DHCP از MADCAP درخواست IP می کنند.
MADCAP هم یک پروتکل است مثل DHCP.

مثلاً فرض کنید که Server دارای یک کارت شبکه ی خاص است که داده های ویدیویی را دریافت می کند و قصد دارد آنها را میان یکی از دو گروه زیر Share کند:

- برخی Client های در DHCP Server تعیین می کنیم.
- همه ی Client هایی که آدرس Multicast IP سرور را دارند.

برای ایجاد یک Multicast Scope بر روی آبجکت IPv4 کلیک راست کرده و گزینه ی New Multicast Scope را می زنیم.
یک رنج که میان محدوده ی D Class باشد تعریف می کنیم و تا پایان پیش می رویم.

Superscope :

گاهی شرایطی وجود دارد که :

- شبکه دارای چندین Subnet مختلف می باشد و می خواهیم همین DHCP Server به همه ی Subnet ها آدرس دهی کند؛
- می خواهیم DHCP Server به کلاینت های Subnet خود، از چندین Range آدرس دهی کند.

در این حالات باید Scope جدید را ایجاد کنیم، سپس Scope قبلی را همراه با Scope جدید، در یک Super Scope قرار دهیم.

برای راه اندازی آن:

1. فرض کنید دو Scope به نام های SCP1 و SCP2 داریم که دارای رنج های زیر هستند:
   SCP1 : از 10.0.1.1 تا 10.0.1.50
   SCP2 : از 10.0.2.1 تا 10.0.2.50
2. برای ایجاد Superscope به سادگی می توان بر روی آبجکت IPv4 کلیک راست کرد و New Superscope را زد.
   اما می توان در PowerShell هم دستور زیر را وارد کرد:

```
Add-DhcpServerv4Superscope -SuperscopeName Super1 -ScopeId 10.0.1.0,10.0.2.0
```

DHCP Backup :

بطورپیشفرض Database مربوط به DHCP Server در مسیر و فایل زیر قرار دارد:

C:\Windows\System32\dhcp\dhcp.mdb

همچنین بطورپیشفرض خود سیستم از خودش Backup تهیه می کند که آن را در مسیر زیر قرار می دهد:

C:\Windows\System32\dhcp\backup

بطورخودکار هر 60 دقیقه یکبار، از تمامی اطلاعات Database مربوط به DHCP، شامل Scope ها، Leased Address ها، Reserved Address ها و .... Backup تهیه می شود.

اما برای تهیه ی دستی Backup از DHCP مربوط به یک Server، کافی ست در کنسول DHCP در کادر سمت چپ، بر روی نام سرور، کلیک راست کرده و Backup را بزنیم، و برای Restore کردنِ آن، به همین شکلل عمل کرده، فقط گزینه ی Restore را انتخاب می کنیم.

از طریق PowerShell :

```
Backup-DhcpServer -Path c:\New Folder
```

```
Restore-DhcpServer -Path c:\New Folder
```

برای تنظیم زمانبندی جهت Backup گیری از DHCP :

```
Set-DhcpServerDatabase
```

IPv6 Process :

به طور کلی به دو طریق می توان به یک Client آدرسی دهی version 6 را انجام داد:

- ❖ Stateful Auto configuration : یعنی آن را محول به DHCP Server کنیم.
  در این حالت باید گزینه ی DHCP IPv6 Stateless Mode را غیرفعال کنیم.

- ❖ Stateless Auto configuration : یعنی آن را محول به Router متصل به Client کنیم.
  در این حالت باید گزینه ی DHCP IPv6 Stateless Mode را فعال کنیم.

فرآیند اختصاص یک IPv6 Address به یک Node در شبکه، SARR نام دارد:

- **Solicit** (مشابه Discover): یک Client برای دریافت IPv6، یک پیام Multicast با یکی از آدرس های زیر را در شبکه ارسال می کند.
  FF02::2 : برای اینکه از نزدیکترین Router در دسترس، درخواست IP کند.
  FF02::1:2 : برای اینکه از نزدیکترین DHCP Server ای که نقش Router را گرفته و در دسترس است، درخواست IP کند.

- **Advertise** (مشابه Advertise): Router یا DHCP Server، بخش Subnet prefix خودش را که 64 بیتی ست، همراه با یک Flag برای او ارسال می کند.
  این Flag که به جهت اعلام 64 بیت مربوط به Interface suffix بکار می رود، یکی از سه حالت زیر را می تواند داشته باشد:
  - A (Autonomous):
    - قابلیت SLAAC را که فراخوانی شده است، Client باید از آدرس MAC خودش که 48 بیت دارد، استفاده کند.
    - اما هنوز 16 بیت برای آدرس IP مورد نظر برای Client ناقص است! پس پروتکلی به نام EUI-64 نیز دست به کار می شود.
    - برای این 16 بیت، از عدد FFFE که بطور قراردادی در سیستم ها تعریف شده است، به صورت زیر استفاده می شود:
      - ○ ابتدا آدرس MAC را به دو نیمه تقسیم می کنیم و عدد FFFE را میان این دو بخش قرار می دهیم و 64 بیت تکمیل می شود.
      - ○ اما حال باید یک بیت از این Interface suffix را معکوس کنیم، هفتمین بیت از سمت چپ.
      - ○ یعنی اگر صفر بود به یک، و اگر یک بود به صفر تبدیل شود.

مثال: فرض کنید Mac Address یک Client برابر است با : aa:e3:2f:10:35:64
پس ابتدا به صورت مقابل در می آید: **aae3:2fff:fe10:3564**
همانطور که می دانیم هر Quartet دارای 16 بیت است، پس هفتمین بیت از چپ، باید در Quartet اول باشد، یعنی aae3
از آنجایی که A برابر با 10 است، پس دو عدد Quartet اول برابر می شوند با: 1010 1010
پس از معکوس کردن هفتمین بیت، Interface suffix به صورت مقابل در می آید: **a8e3:2fff:fe10:3564**

- M (Managed):
  - DHCP Server جهت تعریف 64 بیت مربوط به Interface suffix بکار گرفته می شود.در حقیقت Client ها از هیچ DHCP Server ای IPv6 دریافت نمی کنند، اما می توانند برای تنظیمات بخش Interface suffix از آنها کمک بگیرند.

- O (Other):
  - از طریق ترکیبی از دو قابلیت قبلی، بخش Interface suffix تولید می شود.

- **Request** (مشابه Request در IPv4): پس در صورتی که Flag دریافتی از نوع M باشد، یک پیام Request به DHCP Server شبکه ارسال خواهد شد.
- **Reply** (مشابه Acknowledge در IPv4): DHCP Server آدرس نهایی را تأیید و ارسال می کند.

IPv6 Lease Duration :

این مدت زمان برای IPv6 کاملاً مشابه با سیستم IPv4 است، که شامل دو مشخصه ی متفاوت است:

- **Renew :**

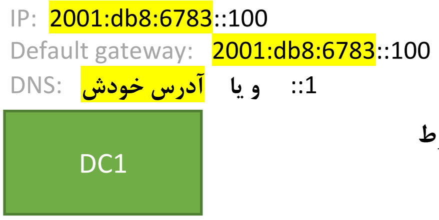
پس از گذشت نیمی از Lease Duration یک درخواست تمدید از طرف Client به همان DHCP Server ارسال می شود.

- **Rebind :**

اگر با ارسال درخواست Renew هیچ پاسخی از DHCP Server نیامد، پیام Rebind در تمام شبکه و برای هر DHCP Server موجود ارسال می شود.

اگر هیچ یک از این دو مراحل، موفقیت آمیز نباشند، همه ی مراحل SARR از ابتدا انجام می شوند.

IPv6 Addressing :



فرض کنید یک DC در شبکه به شکل مقابل داریم.
ابتدا برای تنظیم کردن دستی این IP های ورژن 6، به Ethernet Properties و تنظیم مربوط به IPv6 رفته و حالت دریافت آدرس را از ..obtain an IPv6 autom به حالت ..Use the folliwing تغییر داده و IP ای که در بالا، برای آن درنظر گرفته ایم را وارد می کنیم.

همانطور که می بینیم، خود DC1، هم به عنوان Router و هم به عنوان DNS Server در نظر گرفته شده است.
همانطور که می بینیم، Subnet prefix آنها کاملاً یکسان و برابر با 64 است.

- تنظیم IP را می توان در PowerShell هم از طریق دستور زیر انجام داد:

```
New-NetIPAddress -InterfaceAlias "ethernet0" -IPAddress 2001:db8:6783::100 -PrefixLength 64 -DefaultGateway
2001:db8:6783::100
```

- برای اینکه یک Server بتواند به عنوان یک Router، آدرس Subnet prefix اش را با دیگران Share کند، ابتدا باید قابلیت Advertising را برای او فعال کرد؛ پس در PowerShell آن سیستم (DC1)، دستور زیر را درج و وارد می کنیم:

```
Set-NetIPInterface -AddressFamily ipv6 -InterfaceAlias "Ethernet0" -Advertising Enabled
```

- برای مشخص تر شدن وضعیت می توانیم دستور زیر را وارد کنیم:

```
Get-NetRoute -InterfaceAlias "ethernet0" -AddressFamily ipv6
```

- می بینیم که آن IP ای که عدد 128 را به عنوان prefix قرار داده است، IP خود DHCP Server در همین سیستم می باشد. و Subnet prefix ای که برای Client ها در نظر گرفته است را با عدد 64 بعنوان prefix درج کرده است.

- حال باید یک NetRoute جدید در همین سیستم ایجاد کرده و در شبکه Publish کنیم که Client ها بتوانند برای دریافت Subnet prefix از طریقِ آن با این DC1 ارتباط برقرار کنند.
پس توسط آدرس Subnet prefix همراه با عدد Prefix آن، دستور زیر را درج می کنیم:

```
New-NetRoute -DestinationPrefix 2001:db8:6783::/64 -InterfaceAlias "ethernet0" -Publish Yes
```

نکته: وقتی Publish را به این شکل برابر با Yes قرار دهیم، بطور خودکار، Flag برابر با A خواهد بود.

اما اگر این Error را داد که از قبل این Route موجود است، پس باید آن را توسط دستور زیر پاک کرده و دوباره دستور بالا را امتحان کنیم:

```
Remove-NetRoute -DestinationPrefix 2001:db8:6783::/64 -InterfaceAlias "ethernet0"
```

- حال برای تست اینکه آیا Client ها از سرور DC1، آدرس IPv6 دریافت می کنند، کافی ست در هریک از آنها ipconfig را امتحان کرده و Subnet prefix ها را مقایسه کنیم.

در لیست نتیجه ی دستور ipconfig، یک آدرس v6 دیگر، در زیر آدرس v6 ای که از DC1 دریافت شده است، نشان داده می شود به نام Temporary IPv6 !
این آدرس، یک آدرس موقت برای ارتباط با محیط خارج از Router شبکه است، که مدام تغییر می کند.

IPv6 Setting in DHCP Server :

اگر بخواهیم flag را برابر با M قرار دهیم که یک DHCP Server در شبکه را مسئول تنظیم Interface suffix های IPv6 ها کنیم:

- در DC1، وارد کنسول DHCP شده و روی IPv6 کلیک راست کرده و New Scope را می زنیم.
- یک نام برای آن انتخاب می کنیم.
- Subnet prefix را تا دو نقطه، وارد می کنیم(بصورت ::2001:db8:6783)
- عدد Preference یک عدد جهت اولویت بندی DHCP Server های شبکه ست، و هرقدر این عدد بزرگتر باشد، DHCP Server برای دریافت درخواستهای Interface suffix، در اولویت تر است. (فعلا صفر)
- در تب Add Exclusions می توان به سادگی IP هایی را جدا کرد، مثلاً 2001:db8:6783::100
- حال باید دو زمان را مشخص کنیم:
  - Preferred Life Time : مدت زمانی که طی آن، کاملاً مطمئن به ثابت نگه داشتن IP های Client ها هستیم.
  - Valid Life Time : زمانی که در آن تغییر یا renew کردن IP می تواند انجام شود.، اما اجباری نیست.
- و آنرا فعال کرده و تمام!
- می بینیم که Scope ID برای IPv6 همان Subnet prefix آن است!

- حال که Scope موردنظر ایجاد شده است، باید یک DNS Server Address را برای آن مشخص کنیم.

پس بر روی Scope Option آن کلیک راست کرده و Configure Options را زده و گزینه ی DNS Recursive Name Server IPv6 Address List را فعال کرده و در پایین و نوار New IPv6 Address ، آدرس همان DC1 را، یعنی 2001:db8:6783::100، درج و Add کرده و OK!

- می دانیم که تا اینجا این DC1، مثل یک Router عمل کرده و Subnet prefix را در اختیار Client ها قرار می دهد.
- حال برای اینکه این Server بتواند توسط DHCP Server، تنظیمات Interface suffix را نیز به عهده بگیرد، در PowerShell دستور زیر را درج و وارد می کنیم:

```
Set-NetIPInterface -AddressFamily IPv6 -InterfaceAlias "ethernet0" -ManagedAddressConfiguration Enabled
```

High Availability :

فرض کنید در یک شبکه دو یا چند **DHCP Server** داریم.

یکی از **DHCP Server** ها دچار مشکل شده و از کار می افتد.پس یکی از **DHCP Server** های دیگر باید کار او را انجام دهد.

نکته: فقط می توانیم برای **Scope** های **IPv4** در یک **DHCP Server** دیگر، **Failover Clustering** تشکیل دهیم.

پس برای اینکه در صورت بروز هرگونه مشکل، **DHCP Server** همچنان در دسترس و قابل سرویس دهی باقی بماند، می توان از هریک از روش های زیر استفاده کرد:

Splitted Scope :

باید قبل از اینکه هرگونه اتفاقی بیفتد، یک **Scope** مشترک بین دو یا چند **DC** ایجاد کرده باشیم و آن را بین آنها **Splitt** کرده باشیم.

ابتدا در کنسول **DHCP Server** مربوط به **DC1** در کادر سمت چپ و بالا، بر روی **DHCP** کلیک راست کرده و از طریق **Add Server**، آبجکت مربوط به تنظیمات **DC2** را اضافه می کنیم.

1. **در تنظیمات DC2 یک Scope ایجاد می کنیم، با یک نام و یک محدوده ی دلخواه:**
   - مثلاً با فرض اینکه **DC2** یک **NIC** با آدرس **10.0.0.20** دارد: از **10.0.0.20** تا **10.0.0.250** و با عدد **24** به عنوان **length**.
   - **Default Gateway** را نیز **10.0.0.20** و برای **DNS Server Address**، آدرس **DNS Server** اصلی شبکه را درج می کنیم.
   - چون قصد داریم که این **Scope** را **splitt** کنیم، فعلاً آن را **activate** نمی کنیم و ویزارد را به پایان می رسانیم.
2. **حال Scope ایجاد شده را split می کنیم.**
   - بر روی آن کلیک راست کرده و گزینه ی **Advanced** و سپس **Split-Scope** را می زنیم.
   - سروری که قرار است این **Scope** را مشترک شود، **Add** می کنیم.(**DC1**)
   - محدوده ی هریک از **Split** ها را مشخص می کنیم.
   - میزان تأخیر هریک از **DHCP Server** ها برای پاسخگویی به **Client** ها تعیین می کنیم که می توان برای **Host** (**DC2**) مقدار صفر و برای **Added** (**DC1**) مقدار **500** را تعیین کرد و تمام!
3. **هریک از Split ها را در هریک از DHCP Server ها Activate می کنیم.**(کلیک راست و **Activate**)

نکته:

هرتغییری در هریک از **Split** ها در **DHCP Server** خودشان که رخ بدهد، در **DHCP Server** دیگری، **replicate** یا **update** نمی شود، به جهت جلوگیری از تداخل میان آدرس دهی ها.

نکته:

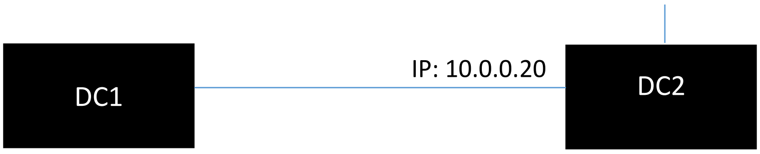
این روش، به خوبی عمل می کند، اما با این شرط که مدت زمان **Down** بودن سرور **down** شده، بیش از یک حدی نباشد.

: Load Sharing

بار کاریِ شبکه را بین دو DC، Share می کنیم.

هر دو DC فعال بوده و بین آنها مدام عملیات Replication انجام می شود که در نتیجه هردو DC با هم Sync خواهند بود.

با فرض اینکه DC2 سیستم DHCP Server اصلی شبکه است، که دارای چند NIC و چند DHCP Scope است، قصد داریم work load را برای یکی از Scope های آن، با DC1، تقسیم کنیم.



- **ابتدا در DC1 یک Scope ایجاد می کنیم.**
- **با فرض اینکه DC2 یک NIC با آدرس 10.0.0.20 دارد: از 10.0.0.20 تا 10.0.0.254 و با عدد 24 به عنوان Net Mask.**
  برای Default Gateway آدرس 10.0.0.20 و برای DNS Server Address، آدرس DNS Server اصلی شبکه را درج می کنیم.
- **و آن را فعال نگه داشته و Finish!**

- **اگر بخواهیم بر روی تمامی Scope های شبکه، این عملیات را انجام دهیم، بر روی آبجکت IPv4 کلیک راست کرده و Configure Failover را می زنیم.**
- **اما اگر بخواهیم فقط بر روی همین Scope ای که در محدوده ی 10.0.0.0 است، انجام دهیم، بر روی این Scope کلیک راست کرده و Configure Failover را می زنیم.**
- **Server دوم را انتخاب می کنیم.**

در تب Create a new failover Relationship. یک زمان را برای Maximum Client Lead Time تعیین می کنیم:

- **فرض کنیم زمانی که DHCP Server اول به Client1 آدرس IP ای داد و ناگهان قبل از اینکه به DHCP Server دوم اعلام کند که فلان IP را به این Client1 داده ام، ارتباطشان قطع شود.**

❖ **پس DHCP Server دوم کنترل را بدست می گیرد، اما اطلاع ندارد که آن IP، به Client1 اختصاص داده شده است، پس احتمال می رود که آن IP را به کلاینتی دیگر اختصاص دهد، که در اینصورت Conflict رخ می دهد.**

❖ **پس وقتی DHCP برای اولین بار به یک Client یک IP می دهد، باید به اندازه ی این مدتی که تعیین می کنیم، صبر کند که اگر توسط درخواست یک Client دیگر، تداخلی پیش نیامد، کاملاً طبیعی به کارش ادامه بدهد.(مثلاً 5 دقیقه)**

- **برای Mode، گزینه ی Load Balance را می زنیم.**
  - **می توانیم میزان تقسیم Load کاری شبکه را میان Server ها بر حسب درصد تعیین کنیم.**
- **گزینه ی ..State Switchover Perc را رها می کنیم.**
- **برای Shared Password یک پسورد تعیین می کنیم، که باعث برقراری یک ارتباط امن میان Server ها می شود.**
- **و تمام!**
- **برای تستِ آن، می توان مثلاً یک Reservation Address ایجاد کرد.**

نکته: برای replicate شدن سریع تر آن، می توان روی Scope آن کلیک راست کرده و replicate Scope را زد.
حال هراتفاقی که در این Scope و در هر یک از DC ها بیفتد، در Server دیگر هم update می شود.

- **برای نحوه ی عملکرد Maximum Client Lead Time، می توانیم یکبار یکی از Scope ها را حذف کرده و DHCP Backup را Restore کنیم تا ببینیم که به جهت این گزینه، Scope های Restore شده، به طور سریع به کار نمی افتند.**

Hot Standby :

در این روش یک **DC** فعال داریم که بار کاری شبکه را به دوش می کشد که **Primary Server** نامیده می شود، و یک **DC** داریم که در حالت غیرفعال قرار دارد، و به آن **Active Standby** گفته می شود.
یعنی هر دو سیستم مدام بایکدیگر **replicate** می شوند، اما تمام سرویس دهی، فقط توسط یکی از آنها انجام می شود، و دیگری مثل یک جایگزین آماده باش در شبکه قرار می گیرد.

- ابتدا در **DC1** یک **Scope**، مشابه **Scope** بالا، ایجاد کرده و وارد **Configure Failover** آن می شویم.
- گزینه ی **..Reuse existing failover relat** نباید فعال باشد.
- در تب **Create a new failover Relationship** ، برخی گزینه ها مشابه به حالت قبل هستند.
- برای **Mode**، گزینه ی **Hot Standby** را انتخاب می کنیم.
- گزینه ی **Addresses reserved for standby Server** چند درصد از آدرس ها را برای سرور **Standby** ذخیره می کند.
- گزینه ی **state switchover Interval**، تعیین می کند که چند دقیقه پس از **down** شدن سرور اول، سرور دوم **Run** شود.

نکته : باید دقت کرد که کدام Server در نقش Standby قرار دارد!

MAC Address Filtering (Layer 2 Filtering) :

در حقیقت جهت جلوگیری از نفوذ هکرها، باید کاری کنیم که تنها سیستم هایی که می شناسیم، از DHCP آدرس IP دریافت کنند. و یا اینکه گاهی می خواهیم یکی یا تعدادی از Client ها، از DHCP آدرس دریافت نکنند، پس دسترسی آنها به DHCP Service را Block می کنیم.
همانطور که می دانیم در Link Layer ، نوع ارتباطات بر اساس یک آدرس 12 کاراکتری به نام آدرس فیزیکی می باشد.
پس این کار را توسط دو لیست به نام های Allow و Deny در DHCP Server و به کمک MAC Address های دستگاه ها انجام می دهیم.

این دو لیست در زیرمجموعه ی پوشه ی Filter در کادر سمت چپ کنسول DHCP قرار دارند که بطور پیشفرض غیرفعال هستند.
برای فعال سازیِ آنها وارد Properties آبجکت IPv4 شده و در تب Filters آنها را فعال می کنیم و یا به سادگی بر روی آنها کلیک راست کرده و Enable را می زنیم.
اما وقتی که این دو لیست فعال شدند، تا زمانی که لیست Allow خالی باشد، یعنی به هیچ Client ای هیچ IP اختصاص نمی دهد!
برای اضافه کردن Client ها به این List، باید MAC Address هریک از Client ها را پیدا کرده و بر روی Allow کلیک راست و New Filter را زد و آن را بدون علامت های dash درج و Add کرد.مثلاً : C29FFEA03000

اگر هم بخواهیم از Client هایی که آدرس IP دریافت کرده اند، عملیات Filtering را روی آنها اعمال کنیم، کافی ست در بخش Address Leases، Client یا Client های موردنظر را انتخاب کرده و کلیک راست کرده و Add to Filter را بزنیم.

همانطور که می دانیم، شش رقم یا کاراکتر اول یک آدرس فیزیکی، شناسه ی شرکت سازنده ی آن دستگاه می باشد که در همه ی دستگاه های تولیدیِ آن شرکت، یکسان و ثابت است.
برای اینکه در لیست Allow تعیین کنیم که هر دستگاهی که دارای Mac Address ای با شناسه ی سازنده ی مورد نظر وارد شد، بتواند IP دریافت کند، کافی ست در پنجره ی New Filter فقط همان شش کاراکتر اول را همراه با یک * درج و Add کرد. مثلاً : C29FFE*

Add-DhcpServerv4Filter

در حقیقت با فعالسازی DHCP Filtering، بطور پیشفرض همه ی آدرس ها allow هستند، اگر آدرسی را نیز allow کنیم هم allow خواهد بود!

:FSMO Rules (Flexible Single Master Operation)

دو Role اول، چون فقط در سطح Forest کار می کنند، Forest Base نامیده می شوند.
برای مشاهده ی آنها، وارد پنجره ی AD domains and Trusts شده و روی AD Domains and Trusts کلیک راست کرده و Operations master را می زنیم.

: Schema Master

- در یک Forest، فقط یک Schema Master وجود دارد.
- اولین Role که در Forest نصب می شود، Schema Master خواهد بود.
- این Role در ریشه ی جنگل، یعنی اولین دامینی که در Forest ایجاد شده است، قرار دارد.
- ساختار آن، ثابت و تغییر ناپذیر نیست.
- در صورت ایجاد تغییر در ساختار schema master این Role تغییرات را در سطح جنگل، replicate می کند.
- از وظایف آن، انجام Replication بین Domain هاست.
- قابلیت این را دارد که برای مدتی offline باشد.

: Domain Naming Master

- در یک Forest، فقط یک Domain Naming Master وجود دارد.
- این Role در ریشه ی جنگل، یعنی اولین دامینی که در Forest ایجاد می شود قرار دارد.
- از وظایفِ آن، اضافه یا حذف کردن Domain ها و تنظیم یا تأیید نام و مشخصات آنها در درون Forest می باشد.
- مثلاً اگر شما یک Domain جدید را در Forest موجود ایجاد می کنید، این Role تضمین می کند که چنین نام Domain ای قبلاً وجود نداشته باشد.
- اگر Domain Naming Master به هر دلیلی از کار بیفتد، نمی توانید Domain جدید ایجاد کنید.
- قابلیت این را دارد که برای مدتی offline باشد.

نکته: سه Role دیگر، چون در سطح Domain کار می کنند، به اصطلاح Domain Base نامیده می شوند.
برای مشاهده ی آنها در AD User and Computers روی Root Domain کلیک راست کرده و Operations master را می زنیم.
از این سه Role، فقط یکی از آنها می تواند Offline کار کند، که RID Master است!

: (Relative ID) RID Master

- در یک Domain، فقط یک RID Master وجود دارد.
- به محض ایجاد یک Domain یک شماره ID یکتا برای آن ایجاد می شود که RID Master نام دارد.
- هر آبجکت در AD، دارای یک شماره ی یکتا به نام SID است که چند رقم آخر آن، بخش نسبی است.
- به منظور جلوگیری از ایجاد چند SID یکسان، RID Master پدید آمد، که به محض ایجاد یک Object، فوراً از RID Master، یک SID دریافت می کند.
- به منظور ارتباط منظم و صحیح میان Domain ها، به این ID نیاز است.

: Primary Domain Controller (PDC) Emulator

- از وظایف مهم آن، Synchronize کردن زمان در Root Domain و replicate کردن آن با همه ی Domain هاست.

- از دیگر وظایفِ آن مدیریت و **Replication** مربوط به **Password** ها در سطح **Domain** می باشد.
- از دیگر وظایفِ آن، این است که کلیه ی **Policy** های اعمال شده در **Group Policy** مربوط به یک **Domain** را در سطح جنگل، **replicate** می کند.
- زمانی که یک **GPO** ساخته می شود، در پوشه ی **sysvol** قرار می گیرد و این پوشه محتویات خود را با **PDC Emulator** به اشتراک می گذارد. پس به محض اینکه در یکی از دامینهای جنگل، **GPO** ایی ساخته می شود و یا تغییراتی در آن اعمال
- می شود، کلیه ی اطلاعات آن در اختیار **PDC** قرار می گیرند و **PDC** آنها را با دیگر **Domain** های جنگل، **Replicate** می کند.
- بطور اکید توصیه می شود که این **Role** خاموش نباشد و یا حداقل برای زمانی طولانی **offline** نباشد!

: Infrastructure Master

- زیرساخت میان **Domain** ها و **Domain Controller** ها را کنترل و **maintenance** می کند.مثلاً ایجاد یا حذف یک **Domain** را به اطلاع **Domain** های دیگر می رساند.
- توصیه می شود که **Online** باشد.
- توصیه ی می شود که نباید **Infrastructure master** و **Global Catalog** بر روی یک **DC** نصب شوند!
- وقتی که **Infrastructure Master** بخواهد خودش را **update** کند، اطلاعاتش را با **Global Catalog** مقایسه می کند و چون هر دو آنها روی یک **DC** هستند و **Global Catalog** قبلا آپدیت شده است، **Infrastructure Master** دیگر خودش را آپدیت نمی کند! در نتیجه اطلاعاتش را با دیگر **DC** ها **replicate** نمی کند!
- اما اگر همه ی **DC** ها دارای **Global Catalog** باشند، دیگر مشکلی پیش نمی آید، زیرا در این صورت همه ی **Global Catalog** ها اطلاعات آپدیت شده را دارند، که در این صورت، **Infrastructure Master Role** دیگر کار نمی کند!
- پس این **Role** در دو حالت کار نمی کند:
- زمانی که تمام **DC** ها دارای **Global Catalog** باشند.
- زمانی که **Forest** دارای فقط یک **Domain** باشد.

پس چنانچه یک DC جدید راه اندازی کنیم که شامل Global Catalog هم نباشد، Infrastructure Master را به آن جابجا می کنیم.

می توان نقشهای **FSMO** را از یک **DC** به **DC** دیگر منتقل کرد.

انتقال این **Role** ها در دو حالت صورت می پذیرد:

- **Transfer** : هنگامی که در موقع حیات **DC** اول، می خواهیم نقش ها را به **DC** دوم انتقال دهیم؛ به دلایلی مثل قوی تر بودن **DC** دوم و یا ارتقاء سیستم عامل.
- **Seize** : هنگامی که **DC** اول که دارای این نقش ها بوده، از بین رفته است و حال می خواهیم نقشها را روی یگ **DC** دیگر داشته باشیم.

Transfer the FSMO Roles :

در ابتدا لازم است که روی سیستم جدید، یک Win Server نصب و به شکل یک ADC آن را به Root Domain متصل کنیم.

فرض کنید که می خواهیم دقیقاً ببینیم که هریک از این Role ها بر روی کدام Server کار می کنند، پس به cmd رفته و دستور مقابل را وارد می کنیم:

Netdom /query fsmo

برای انتقال Schema Role:

- **در Run درج می کنیم mmc.exe تا پنجره ی کنسول مدیریتی snap-ins باز شود.**
- **از منوی بالا File را و سپس Add or Remove Snap-in را می زنیم.**
- **اگر در سمت چپ پنجره ی باز شده، گزینه ی Active Directory Schema نباشد، باید فایل dll آن را رجیستر کرد.**
- **برای این کار cmd را باز کرده و درج و Enter می کنیم: regsvr32 schmmgmt.dll**
- **حال گزینه ی Active Directory Schema را انتخاب و Add کرده و OK.**
- **پس روی گزینه ی [...] Active directory Schema کلیک راست کرده و change AD DC را می زنیم.**
- **در لیست پایین، DC مقصد را انتخاب و ok می کنیم.**
- **حال دوباره روی گزینه ی [...] Active directory Schema کلیک راست کرده و اینبار operations master را می زنیم.**
- **و بالاخره روی Change زده و تمام!**

برای انتقال Domain Naming Master:

- **پنجره ی AD Domains and Trusts را باز کرده و در سمت چپ روی AD Domains and Trusts کلیک راست کرده و**
- **change AD DC را انتخاب می کنیم.**
- **در پنجره ی باز شده، DC مقصد را انتخاب کرده و OK.**
- **حال دوباره روی AD DC کلیک راست کرده و اینبار Operations master را می زنیم.**
- **و change را زده و تمام!**

برای انتقال هر سه نقش Domain Base:

از طریق GUI :

- **به Active directory users and computers رفته و در سمت چپ، روی AD Users and Computers کلیک راست و گزینه ی Change Domain Controller را زده و DC مقصد را انتخاب و OK می کنیم.**
- **حال بر روی گزینه ی Root DC کلیک راست و Operations Master را زده و تک به تک برای هر سه Role ، گزینه ی Change را می زنیم و تمام!**

نکته : اگر این Role ها را به یک DC دیگر منتقل کردید و به هر دلیلی دوباره برگردانید به DC قبل، به احتمال خیلی زیاد، قابلیت Replicate شدن و قابلیت های دیگر را از دست می دهند.مخصوصاً RID Master ، که باعث مشکلاتی می شود مثل عدم توانایی ایجاد User جدید!

نکته : Role های Operation Master ، قابل پیاده سازی روی RoDC نیستند، چون نیاز به دسترسی writable به Object ها و Attribute های دامین و Forest دارند.

و یا از طریق PowerShell :

```
Move-ADDirectoryServerOperationMasterRole -Identity "PC2" -OperationMasterRole PDCEmulator
Move- ADDirectoryServerOperationMasterRole -Identity "PC2" -OperationMasterRole RIDMaster
Move- ADDirectoryServerOperationMasterRole -Identity "PC2" -OperationMasterRole Infrastructure Master
```

: Seize the FSMO Roles

فرض کنیم که DC2 که صاحب همه ی FSMO ها بوده است، ازبین رفته است! حال باید DC1 در دامین payamavar.local این نقش ها را Seize کند یا به قولی بقاپد.
پس در DC1 که قرار است این نقشها را محول شود وارد cmd شده و به ترتیب وارد می کنیم:

1. **Ntdsutil**
2. **Roles**
3. **Connections**
4. **Conncet to server payamavar.local**
5. **Quit**
6. **Seize schema master**
7. **Seize naming master**
8. **Seize rid master**
9. **Seize infrastructure master**
10. **Seize pdc**

نکته:
اگر پس از seize کردن این Role ها، دوباره DC2 به دامین برگشت، به این دلیل است که Role های FSMO همزمان بر روی دو Server نصب هستند که موجب Conflict شدیدی خواهد شد. پس باید از بازگشت آن جلوگیری کرد!

Upgrade the Active Directory:

فرض کنید که در شبکه مان، **main DC**، دارای یک ورژن قدیمی ویندوز **Server** است و می خواهیم آنرا به **Server 2016** ارتقا دهیم.

1. یک ویندوز سرور **2016** نصب و عضو **Domain** می کنیم.
2. **AD DS** را نصب و آن را به عنوان **Add a DC to an existing Forest** و با **functional level** هم سطح با قدیمی ترین ویندوز سروری که در شبکه حضور دارد، تنظیم می کنیم.
3. تمام **FSMO Role** ها را از **main DC** به این ویندوز سرور **2016** انتقال می دهیم.
از آنجایی که **FSMO Role** ها معمولاً همه با هم فقط در یک **DC** می توانند وجود داشته باشند، آنها را منتقل می کنیم.
4. **Active Directory** سرور قدیمی را با دستور زیر در **PowerShell** خودش، حذف می کنیم:

```
Uninstall-ADDSDomainController -DemoteOperationMasterRole –RemoveApplicationPartition
```

(بعد از اجرای دستور از شما برای اکانت **Local Administrator** یک رمز درخواست می کند.)

5. حال اگر **Server** قدیمی تری در شبکه موجود نباشد، **functional level** ویندوز **Server 2016** را ارتقا می دهیم:
نکته: **Domain Functional Level** می تواند بالاتر از **Forest FL** باشد.
نکته: **Forest FL** را می توان فقط ارتقا داد، پایین نمی توان آورد.
نکته: ابتدا **Domain Funtional Lever** و سپس **Forest FL** را افزایش می دهیم.

- روش اول:

در **Server Manager** و **Tools** گزینه ی **Active Directory Administrative Center** را انتخاب کرده و با انتخاب نام **Root Domain** در چپ، در سمتِ راست پنجره، گزینه های **Raise the functional Level** ظاهر می شوند.

- روش دوم:

در **Active Directory Domains and Trusts** در کادر سمت چپ، می توانیم روی نام های **Active Directory Domains and Trusts** و نام **Root Domain** کلیک راست کنیم و آنها را **raise** کنیم.

: Demotion and Deletion a DC

اگر DC ای که حذف می کنید، آخرین و تنها DC یک شبکه (به عبارتی یک Site) است، قبل از حذف آن، تمام کامپیوترهای عضو را یا حذف کنید و یا به یکی دیگر از دامین های آن Forest انتقال دهید. سپس DC را حذف کنید.

- هیچ یک از 5 نقش FSMO نباید روی این سیستم فعال باشند، پس درصورت وجود، باید انتقال یابند.
- با User مدیر، وارد DC مورد نظر شوید.
- اگر قصد دارید که تنها یک Domain Controller از یک Domain را حذف کنید، با یک حساب Enterprise Admins وارد شوید.
- در Server Manager و گزینه ی Manage ، گزینه ی Remove Roles and Features را بزنید.
- تیک گزینه ی AD DS را بردارید.
- Demote this domain Controller را بزنید.
- حدالامکان گزینه ی .. Force the removal of.را تیک نزنید.
- از آنجایی که یک Domain Administrator به local Administrator تبدیل می گردد، از شما می خواهد که password جدیدی برای local administrator انتخاب کنید که بصورت پیشفرض اگر پسورد سابق را هم مجددا وارد کنید، خطایی نمی گیرد.

در پایان باید مطمئن شوید که این کامپیوتر دیگر نقش DC ندارد، حال باید عملیات Metadata Cleanup را انجام دهیم.

البته اگر، بدون انتقال Role های یک DC، آن را Metadata Cleanup کنید، دیگر آبجکتی با آن Replicate نمی کند!

: GUI Metadata Clenaup

همیشه قبل از Metadata Cleanup باید FSMO Roles را در صورت وجود، به یکی از DC های Online و موجود، منتقل کنیم.
در یکی از DC های این شبکه، کنسول Active Directory users and computers را اجرا کنید. DC حذف شده نباید در OU مخصوص Domain Controller ها وجود داشته باشد، اگر هم باشد، باید آن را Remove کرد.

در یکی از DC های این شبکه، کنسول Active Directory Sites and Services را اجرا کنید، در Sites و بعد در زیرگزینه های نام Site (Default-first-site-name) باید در قسمت Servers، نام DC فوق را delete نمایید.

: DOS Metadata Clenaup

اگر قبل از **Metadata Cleanup** نقش های **FSMO** را منتقل نکرده باشیم، در روش **DOS**، پس از حذف فایلهای **Metadata**، این کار انجام خواهد شد، با این تفاوت که اگر قبل از عملیات **Metadata Cleanup** این کار را انجام دهید، اختیار انتخاب **DC** جایگزین با شماست، اما در طی مراحل **Metadata Cleanup**، خود سیستم یکی از **DC** ها را بعنوان میزبان جدید **FSMO Roles** انتخاب خواهد کرد.

1. Ntdsutil
2. Metadata cleanup
3. connections
4. Connect to server <newDCName>
5. Quit
6. Select operation target
7. List domains
8. Select domain payamavar.local و یا <NumberOfDomain>
9. List sites
10. Select site <newDCName> و یا <NumberOfSite>
11. List servers in site
12. Select server <OldDCName>
13. Quit
14. Remove selected server

: Delete a DC

گاهی مجبور به حذف یک **DC** می شویم که اکنون به آن دسترسی نداریم. مثلاً در یک آتش سوزی این **DC** از بین رفته است، اما هنوز اجزای شبکه سعی می کنند به این **DC** مراجعه کنند، پس مشکلاتی پیش می آیند.

چون فایل های **metadata** مرتبط با این **DC** ، هنوز حذف نشده اند و بر روی عملیات **Replication** بین **DC** ها و نیز **DFS Replication** تاثیر می گذارند!

- پس باید بلافاصله بعد از حذف ناگهانی یک **DC** اقدام به حذف فایل های **metadata** باقی مانده از آن **DC** کرد.
- اگر **main DC** بوده است، باید فوراً **FSMO Roles** را به یک **DC** موجود منتقل کنیم.

WDS (Windows Deployment Service):

این سرویس، به ما امکان نصب ویندوز برای چند سیستم بطور همزمان و از طریق شبکه را فراهم می کند. (**PXE Installation**)
به این صورت که یک سیستم **Server** را جهت این سرویس در شبکه، موظف می کنیم، و به آن **WDS Server** گفته می شود.

WDS Server باید شامل موارد زیر باشد:

- باید یک **DNS Server** در شبکه موجود باشد، که الزامی به راه اندازی آن در **WDS Server** نیست.
- باید یک **DHCP Server** در شبکه موجود باشد، که اگر در **WDS Server** باشد، مراحل را ساده تر می کند.
- کارت شبکه ی هریک از **Client** های موجود در شبکه، باید قابلیت **PXE Boot** را پشتیبانی کنند، وگرنه نمی توانند از **WDS Server**، سرویس دریافت کنند.

راه اندازی **WDS Server** :

1. بر روی سیستم درنظر گرفته شده برای **WDS**، ویندوز **Server** را نصب و آن را عضو **Domain** می کنیم.
2. **DHCP Service** را راه اندازی می کنیم.
   - اگر **DHCP Server** در یک سیستم دیگر باشد، باید در کنسول آن، یک **Server option** به نام **option 60 PXE Client** را تنظیم کنیم، که وظیفه ی معرفی **WDS Server** به سیستم ها را برعهده دارد.
   - اما اگر بخواهیم سرویس **DHCP** را نیز بر روی **WDS Server** راه اندازی می کنیم، (که اگر از قبل موجود بوده باشد، می توان توسط قابلیت **Migration**، آن را به این **WDS Server** انتقال هم داد) گزینه ی **option 60** به صورت خودکار ساخته خواهد شد.

راه اندازی **PXE Option 60** (Preboot Execution Environment):

- در کنسول **DHCP**، وارد تنظیمات **Server Option** مربوط به **IPv4** شده و مشاهده می کنیم که گزینه ی **060 PXEClient** یا وجود ندارد و یا غیرفعال است.
- وارد **cmd** شده و دستور **netsh** را وارد می کنیم.
- سپس برای فراخوانی سرویس **DHCP** ، درج می کنیم: **DHCP**
- آدرس یا نام **WDS Server** را به صورت زیر وارد می کنیم؛

```
server 192.168.139.144
```

- برای تنظیم **Option 60** دستور زیر را وارد می کنیم:

```
add optiondef 60 PXEClient String 0 comment=”Option added for PXE Support”
```

- حال باید **value** تنظیمات **option** را وارد کنیم:

```
Set optionvalue 60 string pxeclient
```

- با دستور زیر می توانیم تنظیمات را مشاهده کنیم:

```
show optionvalue all
```

3. ابزار Windows ADK را بر روی WDS Server نصب می کنیم:

- توسط یک Search در Internet تحت عبارت download windows Assessment and Deployment kit، فایلی که لینک آن به نام Download the Windows ADK for Windows 10، در سایت Microsoft وجود دارد را دانلود کرده و وارد مراحل نصب آن می شویم.
  - گزینه ی ...Download the Windows Assessment and Deployment Kit را زده و یک آدرس برای آن مشخص می کنیم. مثلاً : C:\ADK
  - برای ..Send Anonymous u ، گزینه ی No را زده و تا پایان دانلود پیش می رویم.
  - پس از دانلود، وارد محل دانلود آن شده و فایل exe. را باز کرده و اینبار گزینه ی ..Install the Windows Assessment را انتخاب و پیش می رویم.
  - تمام گزینه های تب Select Features را (به جز مثلاً Microsoft SQL Server) انتخاب و نصب می کنیم.

4. Role مربوط به Windows Deployment Services را نصب می کنیم.

5. یک Hard Disk جهت Shared Folder در شبکه، به این WDS Server اضافه می کنیم.

- اگر سیستم فیزیکی است، بهتر است که SSD در نظر گرفته شود.
- وارد Disk Management شده و آن را فعال کرده و نوع آن را GPT قرار داده و آن را تبدیل به یک درایو جدید از نوع NTFS می کنیم.

6. DVD یا Image مربوط به سیستم عامل موردنظر را insert می کنیم.

7. WDS را پیکربندی می کنیم:

- وارد Server Manager شده و در کادر سمت چپ، WDS را انتخاب کرده و در کادر سمت راست، بر روی گزینه ی این Server، کلیک راست کرده و Windows Deployment Services را می زنیم.
- در سمت چپ کنسول، از زیر گزینه ی Servers، بر روی گزینه ی همین Server کلیک راست کرده و Configure Server را می زنیم.
- در ویزارد، Integrated with AD را زده و در تب Remote Folder Location، درایو هارد دیسک جدید را انتخاب و یک نام برای پوشه ی آن درج می کنیم. (مثلاً RemoteInstall)
- در تب Proxy DHCP Server هردو گزینه ی don't listen on IPv6 Ports و ..Configure DHCP Opti را فعال می کنیم.
- در تب PXE Server، برای اینکه بتوانیم به همه ی سیستم های تازه وارد به شبکه سرویس دهی کنیم، گزینه ی
- Respond to all Client را می زنیم، و اگر تعداد Client ها خیلی زیاد باشد و قرار نباشد که یک کاربر کنترل کننده، مراحل نصب و راه اندازی آنها را انجام دهد، گزینه ی Require administrator approval را غیرفعال نگه می داریم و next و Finish!

8. از ویندوز موردنظر، یک Image ایجاد می کنیم.

- از زیرگزینه های آبجکت مربوط به WDS Server، در کادر سمت چپ، بر روی Install Image کلیک راست کرده و Add Install Image را می زنیم.
- یک نام برای image Group درج کرده و سپس برای Image File، از طریق Browse، به درایوی که فایل های نصب سیستم عامل وجود دارند رفته و در پوشه ی Source، فایل install.wim را انتخاب می کنیم.

نکته: اگر این فایل وجود نداشت، وارد cmd شده و دستورات زیر را به ترتیب اجرا می کنیم (D درایو فایل نصب ویندوز است):

dism /Get-WimInfo /WimFile:D:\sources\install.esd

حال در نتیجه ی آمده، احتمالاً برای ورژن های مختلف یک شماره ی Index درج کرده (Data Center یا Standard و ...) توسط آن دستور زیر را نیز وارد کرده و صبر می کنیم:

dism /Export-Image /SourceImageFile:D:\sources\install.esd /SourceIndex:2 /DestinationImageFile:C:\Users\Administrator\Desktop\install.wim /Compress:max /CheckIntegrity

و صبر می کنیم تا این فایل ایجاد شود.

نکته: این فایل را تا پایانِ نصب و راه اندازی همه ی ویندوزها نگه می داریم.

سپس در تب Image File، این فایلی که ایجاد شده است را انتخاب کرده و Next می کنیم.

- در تب بعد، فقط گزینه ی DataCenter را انتخاب کرده و Next و نصب را به پایان می رسانیم.

9. تنظیمات Boot مربوط به نصب ویندوز را ایجاد می کنیم.

- بر روی Boot Image کلیک راست کرده و Add Boot Image را می زنیم.
- در تب Image File دکمه ی Browse را زده و به درایوی که فایل های نصب سیستم عامل وجود دارند رفته و در پوشه ی Source، فایل Boot.wim را انتخاب می کنیم.
- یک نام برای آن درج می کنیم (مثلاً Server2016-Boot) و نصب را به پایان می رسانیم.

10. سرویس WDS را فعال می کنیم.

- در کنسول WDS، در زیرمجموعه ی Servers، بر روی آبجکت این Server کلیک راست کرده و All Tasks و سپس Start را می زنیم.

11. مواجهه با Boot برای نصب ویندوز در Client ها را تنظیم می کنیم.

- دوباره بر روی آبجکت Server کلیک راست کرده و وارد Properties شده و به تب Boot می رویم.
- برای هردو قسمت Known Clients و Unknown Clients، گزینه های ..Always Continue را می زنیم.

12. Client ها را روشن و راه اندازی می کنیم.

نکته: در حقیقت پیش نیاز همه ی Client ها این است که گزینه ی Boot در تنظیمات SETUP آنها بر روی PXE قرار داشته باشد.

- Client موردنظر را، بدون اینکه دارای هیچگونه DVD Rom یا محتویاتی در حافظه اش باشد، بطور فیزیکی به شبکه متصل کرده و آن را روشن می کنیم.

- سپس نصب را تا مرحله ای پیش می برد که باید زبان را انتخاب کرد، سپس وقتی Next را می زنیم، برای حساب کاربری، مشخصات حساب مدیر شبکه را وارد می کنیم، مثلاً : payamavar0\administrator

- و ...

:Unattended Installation Configuration

در صورت وجود ده ها یا صدها سیستم در شبکه، نصب ویندوزها را به صورت **UnAttended** یا بدون مراقب، انجام می دهیم، یعنی تمام مراحل نصب، شامل: انتخاب زبان و فرمت حافظه و ... به صورت خودکار انجام شده و حتی مراحل اتمام نصب و انتخاب نام کامپیوتر و یک **User Name** و متصل کردن کامپیوتر به شبکه ی **Domain** را به صورت خودکار پیش ببرد.

نکته: فرض را بر این می گیریم که تنظیم **Boot** هریک از **Client** ها، بر روی **PXE** قرار دارد.

1. فایل **Install.wim** را از درون پوشه ی **Source** فایل نصبی ویندوز به جایی درون حافظه کپی می کنیم، و یا در کنسول **WDS** از زیرگزینه های آبجکت **Server**، وارد **Install Images** شده و آبجکت ویندوز را انتخاب کرده و بر روی **Image** ای که در کادر سمت راست قرار دارد کلیک راست کرده و **Export Image** را زده و آن را با نامی دلخواه درون درایو **Shared Folder** ذخیره می کنیم.
2. یک پوشه ی خالی درون درایو **Shared Folder** ایجاد می کنیم، مثلاً به نام : **distribution**

3. از گزینه هایی که همراه با **Windows ADK** نصب شده اند، ابزار **Windows System Image Manager** را باز می کنیم.

- در کادر سمت چپ و بالا، بر روی **Select a Distribution Share** کلیک راست کرده و **Create Distribution Share** را زده و پوشه ای که به نام **Distribution** ایجاد کردیم را انتخاب می کنیم.

همانطور که دیده می شود، سه پوشه ایجاد می شوند:

  - **OEM** برای تنظیمات نصب ویندوز خواهد بود.
  - **Out-of-box** برای تنظیمات پس از نصب است.
  - **Packages** برای نصب و راه اندازی **Feature** ها یا **Role** های خاص است.

- در کادر سمت چپ و پایین، بر روی **Select a Windows Image**، کلیک راست کرده و **Select Windows Image** را زده و فایل **Install.wim** که کپی کردیم یا **Image** ای که **Export** کرده بودیم را انتخاب می کنیم.
- می بینیم که دو پوشه ظاهر می شوند:
  - **Components** شامل گزینه های مربوط به تنظیم نصب و راه اندازی ویندوز از ابتدا تا انتهاست.
  - **Packages** شامل گزینه های **Feature** ها یا **Role** های قابل نصب است. معمولاً بطورخاص برای **Server** هاست.

- در حقیقت برای انجام خودکار تنظیمات، ابتدا **Object** های مربوط به هر کار را از پوشه ی **Components** انتخاب و اضافه و تنظیم می کنیم. اما تنظیماتی که تعریف می کنیم، باید درون یک فایل متنی (**XML**) ذخیره شوند که **Answer File** نام دارد.

ما به دو **Answer File** نیاز خواهیم داشت، یکی برای تنظیمات در زمان نصب، مثل زبان و دیسک ها وغیره! و دیگری برای مراحل بعد از نصب: ساخت **User** و غیره.

ایجاد Answer File اول: مراحل نصب ویندوز

- در کادر **Answer File** در وسط، بر روی **Create or Open an Answer File** کلیک راست کرده و **New Answer File** را می زنیم.
- درون پوشه ی **Components** گزینه ی اول، یعنی **Windows PE** را انتخاب کرده و از درون پوشه ی **Components** مربوط به بخش **Windows Image** (پایین سمت چپ)، بر روی گزینه ی زیر، راست کلیک کرده و **Add Setting to Pass 1 Wndws PE** را می زنیم:

amd64_Microsoft-Windows-International-Core-WinPE_...

- حال زیر مجموعه ای که برای Windows PE اضافه شده است را انتخاب کرده و در کادر سمت راست (MS Wndws...) موارد زیر را درج می کنیم:
  - برای InputLocale درج می کنیم: en-us
  - برای SystemLocale درج می کنیم: en-us
  - برای UILanguage درج می کنیم: en-us
  - برای UILanguageFallback درج می کنیم: en-us
  - برای UserLocale درج می کنیم: en-us

زیرگزینه ی این amd64_MS-Wndws... را انتخاب کرده و:

- برای UILanguage درج می کنیم: en-us
- برای WillShowUI درج می کنیم: OnError : یعنی درصورت خطا، به نمای گرافیکی برگشته و از کاربر درخواست می کند.

- دوباره به پوشه ی Components مربوط به بخش Windows Image (پایین سمت چپ) برگشته و گزینه ی زیر را پیدا کرده و از زیرگزینه های آن، بر روی دو گزینه ی DiskConfiguration و WindowsDeploymentServices، راست کلیک کرده و Add Setting to Pass 1 Wndws PE را می زنیم:

Amd64_Microsoft-Windows-Setup_...

- حال که این دو گزینه هم به زیر مجموعه های Windows PE اضافه شده اند، ابتدا بر روی .Disk Config کلیک راست کرده و Insert New Disk را زده و گزینه ی Disk را انتخاب کرده و در کادر سمت راست، درج می کنیم:
  - برای DiskID درج می کنیم: 0
  - برای willWipeDisk درج می کنیم: true

- از زیرگزینه های Disk، ابتدا بر روی Create Partitions کلیک راست کرده و Insert New CreatePartition را زده و با انتخاب آبجکت جدید، در کادر سمت راست:
  - برای Extend درج می کنیم: true
  - برای Order درج می کنیم: 1
  - برای Type درج می کنیم: Primary

- بر روی Modify Partitions کلیک راست کرده و Insert new ModifyPartition را می زنیم و گزینه ی جدید را انتخاب و تنظیم می کنیم:
  - برای Active درج می کنیم: True
  - برای Extend درج می کنیم: False
  - برای Format درج می کنیم: NTFS
  - برای Label درج می کنیم: (یک نام دلخواه) مثلاً: Windows
  - برای Letter درج می کنیم: C
  - برای Order درج می کنیم: 1
  - برای PartitionID درج می کنیم: 1

- در کنسول WDS از زیرگزینه های آبجکت Server، وارد Install Images شده و گزینه ی ویندوز را انتخاب کرده و بر روی Image ای که در کادر سمت راست قرار دارد کلیک راست کرده و Properties را زده و در تب General نگه می داریم.

- حال در کنسول Windows System Image Manager، در ادامه، آبجکت WindowsDeploymentServices را انتخاب کرده و از زیرگزینه هایش، ImageSelection و از زیرگزینه های آن، InstallImage را زده و تنظیم می کنیم:
  - برای FileName درج می کنیم: نام مقابل File name در تب General را درج می کنیم.
  - برای ImageGroup درج می کنیم: نام مقابل Image Group در تب General را درج می کنیم.
  - برای ImageName درج می کنیم: نامی که در بالای تب General قرار دارد را کپی Paste می کنیم.

- حال گزینه ی InstallTo را انتخاب و تنظیم می کنیم:
  - برای DiskID درج می کنیم: 0
  - برای PartitionID درج می کنیم: 1

- حال وارد آبجکت Login شده و زیرمجموعه ی آن یعنی Credentials را انتخاب و تنظیم می کنیم:
  - برای Domain درج می کنیم: نام Domain شبکه را درج می کنیم مثلاً : payamavar.local
  - Password (حساب Admin شبکه) را همراه با نام User درج می کنیم: Administrator

- از منوی بالای برنامه وارد Tools شده و Validate Answer File را می زنیم، که باید در پنجره ی Messages در پایین، سمت راست، No Warnings or Errors ظاهر شود.

- از طریق File > Save Answer File As این پروژه را با نامی دلخواه در مسیر Shared Folder و پوشه ی RemoteInstall و سپس WdsClientUnattend، ذخیره می کنیم. (مثلاً Unattend-Server2016)

1. وارد کنسول WDS و Properties مربوط به آبجکت Server جاری در کادر سمت چپ می شویم.

- وارد تب Client شده و گزینه ی Enable Unattended installation را فعال کرده و با توجه به اینکه WinServer64x را انتخاب کرده بودیم، بر روی Browse مربوط به x64 architecture کلیک کرده و درون پوشه ی Remote Install، وارد پوشه ی WdsClientUnattend شده و فایلی که توسط Wndws Systm Image Manager ایجاد کرده بودیم را انتخاب و OK می کنیم.

- وارد پوشه ی Install Images شده و آبجکت ایجاد شده ی آن را انتخاب کرده و در کادر سمت راست، وارد Properties مربوط به Image شده و در تب General گزینه ی ...Allow image to install in را فعال کرده و وارد دکمه ی Select File شده و Browse را می زنیم.
- به درایو Shared Folder رفته و وارد پوشه ی RemoteInstall و سپس WdsClientUnattendend شده و فایل XML ایجاد شده را وارد کرده و Apply و OK!
- بر روی آبجکت مربوط به Server، کلیک راست کرده و All Tasks را زده و Restart می کنیم.

2. حال می توانیم سیستم های Client ها را روشن می کنیم تا نصب ویندوز به صورت خودکار، آغاز شود.

نکته: در حقیقت همه ی این تنظیمات تا اینجا، برای بیشتر Windows ها یکسان است. (7 و 8 و 10)

ایجاد Answer File دوم: که مراحل پس از نصب ویندوز را نیز خوکار پیش می برد.

حال که Answer File اول ایجاد و تنظیم شده است، می توانیم Answer File دوم را نیز تنظیم می کنیم.

1. دو Object تخصصی یا specialize (4) ایجاد می کنیم:

- در بخش Windows Image، بر روی گزینه ی amd64_Microsoft-Windows-Shell-Setup.. راست کلیک کرده و گزینه ی Add Setting to Pass 4 specialize را می زنیم و می بینیم که آبجکت آن، در بخش Answer File، به 4 specialize اضافه می شود؛ اما می توانیم همه ی زیرمجموعه های این Object را یکی یکی انتخاب و Delete کنیم و فقط خود amd64_Micros.. را نگه می داریم؛ پس آن را انتخاب می کنیم.
- در منوی سمت راست آن تنظیم می کنیم:
  - برای Computer Name درج می کنیم: *
  - برای CopyProfile درج می کنیم: true
  - برای Product Key: سریال GVLK مربوط به ویندوز موردنظر را وارد می کنیم.
  - برای RegisteredOrganization درج می کنیم: Server-
  - برای RegisteredOwner درج می کنیم: Server-
  - برای TimeZone مثلاً درج می کنیم: W. Europe Standard Time
- در بخش Windows Image، بر روی گزینه ی amd64_Microsoft-Windows-UnattendedJoin.. راست کلیک کرده و گزینه ی Add Setting to Pass 4 specialize را می زنیم و می بینیم که آبجکت آن، در بخش Answer File، به 4 specialize اضافه می شود؛ زیرمجموعه ی این Object، یعنی Identification را انتخاب کرده و تنظیم می کنیم:
  - برای JoinDomain درج می کنیم: Payamavar.local
  - برای UnsecureJoin درج می کنیم: True (جهت نامگذاری مرتب و ترتیبی Client ها و عدم ایجاد نام های Random)

  حال زیرمجموعه ی آن، یعنی Credential را انتخاب و تنظیم می کنیم:
  - برای Domain درج می کنیم: Payamavar.local
  - Password را همراه با نام User مدیر شبکه را درج می کنیم: Administrator

  آبجکت Provisioning را delete می کنیم.

2. دو آبجکت Out-of-box experience یا OOBE (7) ایجاد می کنیم:

- در بخش Windows Image، بر روی گزینه ی amd64_Microsoft-Windows-International-Core.. راست کلیک کرده و گزینه ی Add Setting to Pass 7 oobeSystem را می زنیم و می بینیم که آبجکت آن، در بخش Answer File، به 7 oobeSystem اضافه می شود؛ آن را انتخاب کرده و تنظیم می کنیم:
  - برای InputLocale درج می کنیم: en-us
  - برای SystemLocale درج می کنیم: en-us
  - برای UILanguage درج می کنیم: en-us
  - برای UILanguageFallback درج می کنیم: en-us
  - برای UserLocale درج می کنیم: en-us
- در بخش Windows Image، گزینه ی amd64_Microsoft-Windows-Shell-Setup.. را پیدا کرده و از زیرگزینه های آن،
  - یکبار بر روی AutoLogon راست کلیک کرده و Add Setting to Pass 7 oobeSystem را می زنیم،
  - یکبار بر روی OOBE راست کلیک کرده و Add Setting to Pass 7 oobeSystem را می زنیم،
  - یکبار بر روی UserAccounts راست کلیک کرده و Add Setting to Pass 7 oobeSystem را می زنیم،

  می بینیم که آبجکت های آنها، در بخش Answer File، به 7 oobeSystem اضافه شده اند.

  خودِ amd64_Microsoft-Windows-Shell-Setup را انتخاب کرده و تنظیم می کنیم:
  - برای RegisteredOrganization درج می کنیم: Server- (و یا هرنام دلخواه موردنظر)
  - برای RegisteredOwner درج می کنیم: Server- (و یا هرنام دلخواه موردنظر)

- برای TimeZone مثلاً درج می کنیم: W. Europe Standard Time

از زیرمجموعه های آن، AutoLogon را تنظیم می کنیم:

- برای Domain درج می کنیم: Payamavar.local
- برای Enabled درج می کنیم: True
- برای LogonCount درج می کنیم: 5
- برای Username درج می کنیم: Administrator

زیرمجموعه ی آن، یعنی Password را تنظیم می کنیم: پسورد User مدیر

آبجکت OOBE را تنظیم می کنیم:

- برای HideEULAPage و HideLocalAccountScreen و HideOEMRegistrationScreen و HideOnlineAccountScreens و HideWirelessSetupInOOBE درج می کنیم: True
- زیرمجموعه ی آن، یعنی VMModeOptimizations را Delete می کنیم.
- برای آبجکت UserAccounts :
- گزینه ی AdministratorPassword را تنظیم می کنیم: یک پسورد (پسورد Local Admin سیستم است.)
- بر روی DomainAccounts کلیک راست کرده و Insert New DomainAccountList را زده و آدرس Domain را می زنیم.
- بر روی LocalAccounts کلیک راست کرده و Insert New LocalAccount را زده و Local Account را تنظیم می کنیم:
  - می توان یک توضیح برای Description درج کرد: Built-in Account
  - بهتر است که برای DisplayName و Name یک نام یکسان درج کنیم. (مثلاً MyUser)
  - برای Group درج می کنیم: Administrators و یا Users

  از زیرمجموعه ی آن، برای Password، یک رمزعبور تعیین می کنیم.

حال در منوی بالای برنامه، از Tools، گزینه ی Validate Answer File را می زنیم، و اگر خطایی وجود داشته باشد، در تب Messages در پایین، سمت راست ظاهر می شود، که برای رفع آنها، باید روی آن، دابل کلیک کرده و سپس بر روی گزینه ی بالا آمده، درصورت تنظیم اضافه، کلیک راست کرده و Revert Change را بزنیم، و در صورت نقصان، آن را صحیح درج یا اضافه کنیم.
و در پایان دوباره Validation کرده و در صورت صحت تنظیمات، پروژه را Save می کنیم.

دوباره وارد کنسول WDS و Properties مربوط به آبجکت Server جاری در کادر سمت چپ می شویم.

- وارد تب Client شده و بر روی Browse مربوط به x64 architecture کلیک کرده و درون پوشه ی Remote Install، وارد پوشه ی WdsClientUnattend شده و فایلی که توسط XML را دوباره انتخاب و OK می کنیم.
- وارد تب AD DS شده و به جهت نامگذاری مرتب و تعریف شده، باید یک Format برای آن تعریف کنیم.

باید دقت کرد که این نام نمی تواند بیشتر از 15 کاراکتر باشد.

- برای Format، ابتدا یک نام دلخواه را درج درج می کنیم.

Server-%04#

- طبق این فرمت،

Server- : یعنی همه ی نام ها با -Server شروع شوند.

٪ : مابقیِ هرنام به صورت عددی باشد.

0 : از صفر شروع شود.

4 : چهاررقمی باشد.

- پس نام اولین Client به صورت مقابل خواهد شد: Server-0001

DC%31#

- با DC شروع شده و بخش متغیرِ آن، از سه شروع شده و یک رقمی باشد. اولین نام: DC3

دوباره وارد پوشه ی Install Images شده و آبجکت ایجاد شده ی آن را انتخاب می کنیم.

- در کادر سمت راست، وارد Properties مربوط به Image شده و در تب General، وارد دکمه ی Select File شده و فایل XML را انتخاب می کنیم.

اضافه کردن یک Role یا Feature:

اگر بطورمثال بخواهیم برای همه ی Client ها، یک Role یا Feature خاص، مثل IIS را راه اندازی کنیم:

- **در بخش Windows Image، وارد پوشه ی Packages و سپس Foundation شده و بر روی گزینه ی ..amd64_Micro کلیک راست کرده و Add to Answer File را می زنیم.**

  در تب Answer File پوشه های آن همراه با Object آخری، اضافه شده اند. پس Object را انتخاب و تنظیم می کنیم:

  - **می توانیم هرکدام از Feature هایی که در تب سمت راست، نشان داده می شوند را Enable کنیم که نصب شوند.**

  - **مثلاً برای اضافه کردن IIS :**

    گزینه ی IIS-Web-ServerRole را Enable کرده و از زیرمجموعه های آن IIS-WebServer و IIS-WebServerManagementTools را نیز Enable می کنیم.

پروژه را دوباره Save می کنیم.

دوباره وارد کنسول WDS و Properties مربوط به آبجکت Server جاری در کادر سمت چپ می شویم.

- **وارد تب Client شده و بر روی Browse مربوط به x64 architecture کلیک کرده و درون پوشه ی Remote Install، وارد پوشه ی WdsClientUnattend شده و فایلی که توسط XML را دوباره انتخاب و OK می کنیم.**

  دوباره وارد پوشه ی Install Images شده و آبجکت ایجاد شده ی آن را انتخاب می کنیم.

- **در کادر سمت راست، وارد Properties مربوط به Image شده و در تب General، وارد دکمه ی Select File شده و فایل XML را انتخاب می کنیم.**

Driver Installation :

فرض کنید بخواهیم بطور خودکار، پس از نصب سیستم عامل ها و راه اندازی و اتصال آنها به شبکه ی **Domain**، یک سری **Driver** های چند قطعه یا دستگاه عضو در شبکه نیز، نصب شوند.

- پس فایل های **Driver** هریک از آن دستگاه ها را در یک پوشه، جمع آوری کرده و به **Shared Folder** مربوط به **WDS Server** انتقال می دهیم.
- در حقیقت فایل یا فایل های اصلی نصب یک **Driver**، دارای پسوند **.inf** می باشند.

نکته:
درایورها بسته به نوع **CPU** دسته بندی می شوند، که باید بسته به نوع سیستم های **Client** ها، آنها را اضافه کنید.
برای نوع **CPU** ها، سه اختصار وجود دارد:

IA64 = 64 Bit Itanium Plattform
x86 = 32 Bit Intel/AMD Plattform
amd64 or x64 = 64 Bit Intel/AMD Plattform

برای پیدا کردن مدل **CPU** در یک سیستم، وارد **cmd** شده و درج می کنیم:

wmic CPU get Architecture

که یکی از سه نتیجه ی زیر با معانی روبرو را خواهد داشت:

0 = x86
6 = Ia64 : Itanium Processor Familie (IPF)
9 = x64

1. **Package های Driver ها را وارد کنسول WDS می کنیم.**

- وارد کنسول **WDS** شده و بر روی پوشه ی **Drivers** کلیک راست کرده و **Add Driver Package** را می زنیم.
همانطور که می بینیم، به دو صورت می توان هریک **Driver** را تعریف کرد: یا فقط توسط فایل **.inf** و یا پوشه ی کامل آن.
در اینجا گزینه ی پوشه ی کامل را انتخاب کرده و توسط **Browse**، پوشه ای که حاوی همه ی **Driver** هاست را انتخاب می کنیم.
- پس این مرحله ی **Import** را به سادگی به پایان می رسانیم.
- می توانیم یک گروه برای **Driver** ها ایجاد کنیم، و یک نام برای آن درج کنیم.
- فعلاً نیازی به تغییر یا ایجاد فیلتر نیست، پس **Modify the Filters** را غیرفعال می کنیم و تمام!

نکته: برای اطمینان از نصب بدون شرط **Driver** ها، وارد **Driver Group** ای که ایجاد کردیم شده و در تب **General** گزینه ی **Applicability** را بر روی **All driver packages in the Group** قرار می دهیم.
در غیراینصورت، اگر در یکی از **Client** ها، سخت افزار مربوط به **Driver** موجود نباشد، نصب هم نخواهد شد.

2. **Package های Driver ها را به Boot Image هم اضافه می کنیم.**

- وارد پوشه ی **Boot Images** شده و در سمت راست بر روی آبجکت موجود، کلیک راست کرده و **Add Driver Pack. to Image** را می زنیم.
- پس از یکبار **Next**، گزینه ی **Search for Packages** را می زنیم.
- به سادگی نصب را به پایان می رسانیم.

:Pre-Configuration for WDS

همانطور که می دانیم، حتی با نصب ویندوزهای **Client** ها توسط **WDS** و **Answer File** ها، در پایان، زمانی صرف **update** ویندوزها و نصب درایورها خواهد شد. و یا اگر بخواهیم که یک **Feature** خاص، درون آن ویندوز غیرفعال باشد، باید بعد از نصب آنها، اقدام کنیم.
اما ما می توانیم **Image** هایی که درون **WDS** وارد می کنیم را، از قبل توسط دستور **dism** تغییر دهیم که دیگر نیازی به تغییرات آنچنانی در دستورات **Answer File** نداشته باشیم و زمان راه اندازی و **Update** ویندوزهای **Client** ها را کمتر خواهیم کرد.

فرض کنید بخواهیم به ویندوز **Server 2016**، یک سری **Driver** را، و همچنین آخرین **Update** ها را اضافه کنیم.

- یک پوشه در درون حافظه ایجاد می کنیم، مثلاً به نام **mySRV** و در درایو **C**.
- حال درون این پوشه، پوشه ها و فایل زیر را ایجاد می کنیم:
  - پوشه ای به نام **Driver**: حاوی درایورهای موردنظر برای **Client** ها
  - پوشه ای به نام **Image**: حاوی فایل **install.wim**

    نکته: همانطور که می دانیم فایل های wim نیز نوعی Image محسوب می شوند.
  - پوشه ای به نام **Mount**: (خالی)
  - پوشه ای به نام **Update**: (خالی)

نیاز به دستور **dism** خواهیم داشت که بطورکلی، شیوه ی کار آن به شکل زیر است:

dism / نام عملیات **/** دستورِ دریافتِ نام و آدرسِ فایل هدف

- می توانیم توسط یکی از دستورات زیر، نام برخی از عملیات را همراه با توضیحات، مشاهده کنیم:

Dism /?
Get-Command -Module dism

وارد **PowerShell** می شویم (در زیر هم دستورات **cmd** و هم دستورات **PowerShell** آورده شده اند) :

1. **Image** ویندوز را **mount** می کنیم.

- توسط دستور زیر می توانیم اطلاعات در مورد محتوای فایل **install.wim** دریافت کنیم:

```
dism /get-imageinfo /imagefile:c:\mySRV\image\install.wim
```

```
Get-WindowsImage -ImagePath C:\mySRV\Image\install.wim
```

- فایل **install.wim** را توسط دستور زیر، درون همان پوشه ی **Mount**، بارگزاری یا **mount** می کنیم(شماره **Index**: از دستور بالا):

```
dism /mount-image /imagefile:c:\mySRV\image\install.wim /index:X /mountdir:c:\mySRV\mount
```

```
Mount-WindowsImage -ImagePath C:\mySRV\Image\install.wim -Path C:\mySRV\Mount -Index 4
```

پس از دستور PowerShel آن، حالت Online و نیاز به Restart، باید بر روی False باشند.

نکته: می توانیم یکبار به مسیر Mount رفته و فایل ها را مشاهده کنیم، اما باید از مسیر آن خارج شویم تا عملیات دچار مشکل نشود.

- اگر به هردلیلی، سیستم خاموش یا قطع شد، و دوباره آن را روشن و راه اندازی کردیم و خواستیم این مراحل را ادامه بدهیم، نیاز است که دوباره این **Image** را **mount** کنیم، اما اینبار باید دستور **remount** را بزنیم، یعنی دستور بالا را با کلمه ی **Remount**:

```
dism /remount-image /imagefile:c:\mySRV\image\install.wim /index:X /mountdir:c:\mySRV\mount
```

2. فایل های **Driver** های موردنظر را به ویندوز، اضافه می کنیم.

- توسط دستور زیر بررسی می کنیم که چه **Driver** هایی درون این **Image** که **mount** شده است وجود دارند:

```
dism /get-drivers /image:c:\mySRV\mount
```

```
Get-WindowsDriver -Path C:\mySRV\Mount
```

- برای اضافه کردن **Driver** های موردنظر که درون پوشه ی **Driver** قرار دارند، هم می توانیم یکی یکی عمل کنیم، که باید برای

هریک، فایل inf. آنها را به عنوان فایل نصب، آدرسدهی کنیم، و هم می توانیم همه را با هم اضافه کنیم، که برای این روش، نیاز به فرمان /recurse نیز می باشیم، که بگوید همه ی پوشه ها و زیرپوشه ها را برای دریافت فایل های Driver، جستجو کند.

پس همه را یکجا نصب می کنیم:

```
dism /add-driver /driver:c:\mySRV\driver /image:c:\mySRV\mount /recurse
```

```
Add-WindowsDriver -Path c:\mySRV\Mount -Driver c:\mySRV\Driver -Recurse
```

- حال می توانیم دوباره بررسی کنیم و ببینیم که دقیقاً چه Driver هایی اضافه شده اند.
- فرض کنید بخواهیم یکی از Driver ها را از پوشه ی Mount حذف کنیم، دیگر نمی توانیم همه را با هم نصب کنیم، پس مثلاً:

```
dism /remove-driver /driver:C:\mySRV\Driver\Printer\WINX86\E_JF1IYE.INF /image:c:\mySRV\mount
```

3. بسته های آخرین Update را به ویندوز اضافه می کنیم.

- برای دریافت آخرین Update های ویندوز، وارد لینک زیر شده و در قسمت Search درج می کنیم: windows Server 2016

www.catalog.update.microsoft.com

- برای اینکه آخرین و جدیدترین نسخه ها را ببینیم، کافی ست بر روی نام ستون Last Updated یکبار کلیک کنیم.
- برای دانلود هریک از ردیف ها، بر روی Download آن کلیک می کنیم.
- همانطور که می بینیم، فایل های Update دارای پسوند msu. می باشند. آنها را به پوشه ی Update منتقل می کنیم.
- در حقیقت، بسته های Update ای که دانلود می کنیم، به شکل و نام Package اضافه خواهند شد.
- می توانیم برای مشاهده ی Package های موجود در خود Image ای که mount شده است، وارد کنیم:

```
dism /get-packages /image:c:\mySRV\mount
```

```
Get-WindowsPackage -Path C:\mySRV\Mount
```

- برای افزودن یک Package یا همان فایل های Update ای که دانلود کرده بودیم، دستور زیر را وارد می کنیم:

```
dism /add-package /packagepath:c:\mySRV\update /image:c:\mySRV\mount
```

```
Add-WindowsPackage -Path C:\mySRV\Mount -PackagePath C:\mySRV\Update
```

- برای حذف کردن هریک از Package ها، ابتدا باید نام ثبت شده ی آن را در سیستم پیدا کنیم، و توسط نامش، آنرا حذف کنیم:

```
dism /get-packages /image:c:\mySRV\mount
```

- حال نام Package موردنظر را در مقابل Package Identity کپی کرده و در دستور زیر وارد می کنیم:

```
dism /remove-package /packagename:<...> /image:C:\mySRV\mount
```

4. Feature ها یا Service های خاص را فعال می کنیم تا با نصب ویندوز، نصب شوند.

- برای مشاهده ی وضعیت Feature های ویندوز دستور زیر را وارد می کنیم:

```
dism /get-features /image:c:\mySRV\mount
```

```
Get-WindowsOptionalFeature -Path C:\mySRV\Mount
```

- برای مشاهده ی تنها وضعیت یکی از Feature ها با جزییات (مثلاً IIS)، دستور زیر را وارد می کنیم:

```
dism /get-featureinfo /featurename:iis-webserver /image:c:\mySRV\mount
```

```
Get-WindowsOptionalFeature -Path C:\mySRV\Mount -FeatureName iis-webserver
```

- برای فعال کردن یک Feature که وضعیت State آن بر روی Disable قرار دارد:

```
dism /enable-feature /featurename:iis-webserver /image:c:\mySRV\mount /all
```

```
Enable-WindowsOptionalFeature -Path C:\mySRV\Mount -FeatureName iis-webserver
```

- برای غیرفعال کردن یک feature:

```
dism /disable-feature /featurename:iis-webserver /image:c:\mySRV\mount
```

```
Disable-WindowsOptionalFeature -Path C:\mySRV\Mount -FeatureName iis-webserver
```

5. Image را دوباره بسته و ذخیره می کنیم.

- حال باید این Image که mount شده است را دوباره قطع یا unmount کنیم و همچنین باید یک فرمان commit/ اعلام کنیم که تغییرات ایجاد شده، ذخیره و اعمال شوند:

```
dism /unmount-image /mountdir:c:\mySRV\mount /commit
```

```
Dismount-WindowsImage -Path c:\mySRV\mount1 -Save
```

NANO Server Pre-Configuration for WDS :

مراحل تغییرات فایل Install.wim توسط dism را می توانیم برای NANO Server ها هم انجام دهیم.

باید فایل NanoServer.wim را از درون DVD ویندوز، و پوشه ی NANO Server به درون حافظه (پوشه ی mySRV) کپی می کنیم.

پس ابتدا توسط دستور زیر، مشخصات آن را دیده و سپس آن را mount می کنیم:

```
Get-WindowsImage -ImagePath C:\mySRV\NanoServer.wim
```

- پس از mount کردن، می توانیم Package های موجود در آن را ببینیم:

```
Get-WindowsPackage -Path C:\mySRV\Mount
```

- برای افزودن فایل های Update :

```
Add-WindowsPackage -Path C:\mySRV\Mount -PackagePath C:\mySRV\Update
```

- چون Feature ها و Role های NANO Server، به شکل Package درون پوشه ی Packages در DVD ویندوز، وجود دارند، برای افزودن هریک از آنها به فایل NANO Server ای که از درون حافظه mount شده است، به صورت زیر عمل می کنیم (مثلاً IIS):

```
dism /add-package /packagepath:D:\NanoServer\Packages\Microsoft-NanoServer-IIS-Package.cab
/image:c:\mySRV\mount
```

- کاملاً مشابه به حالت معمولی، unmount می کنیم.

دقیقاً همه ی این تغییرات را می توانیم بر روی فایل های vhdx. هم انجام دهیم.

```
Get-WindowsImage -ImagePath C:\mySRV\DC1.vhdx
```

RSAT :

در حقیقت برای کنترل یک Server، ابتدا باید یک سیستم را به شبکه ی آن متصل کرده و سپس توسط ابزارهایی مثل VNC وارد آن شد. اما توسط یک Extension (افزونه) به نام RSAT یا (Remote Server Administration)، بدون نیاز به ورود به سیستم Server، و تنها توسط یک Windows معمولی (مثل 10) می توان آن را کنترل کرد.
به این صورت که خیلی از کنسول های Windows Server (مثل Server Manager)، به ویندوزهای غیر Server اضافه می شوند.

برای دریافت این نرم افزار در گوگل سرچ می کنیم : RSAT microsoft
وارد لینک جدیدترین ...Download Remote Server Administration Tools for و مربوط به Win.10 شده و Download!
جدیدترین نسخه ی WindowsTH-RSAT_WS_x64.msu را دانلود می کنیم.

قبل از نصب، باید:

- اتصال با اینترنت برقرار باشد.
- وارد کنسول Services شده و از Run بودن سرویس Updates مطمئن شویم.

پس از نصب، یکبار Restart می کنیم و سپس برای اطمینان از نصب صحیح، وارد پنجره ی Programs and Features شده و گزینه ی Turn Windows Features on or off را زده و گزینه ی Remote Server Administration Tools را پیدا کرده و باید هرسه زیرگزینه های آن فعال باشند:

- Feature Administration Tools
- Role Administration Tools
- Server Manager

جهت اتصال به Active directory:

```
Install-WindowsFeature RSAT-ADDS
```

برای دسترسی به این ابزارها، در Control Panel وارد گزینه ی Administrative Tools می شویم.
مثلاً برای کنترل Server Manager، آن را باز کرده و وارد Manage و Add Servers شده و Server مورد نظر را Add می کنیم.

```
shutdown -r -t 0
```

- برای باز کردن پنجره ی Computer Management مربوط به یک سیستم دیگر عضو شبکه، کافی ست این کنسول را باز کرده و در کادر سمت چپ و بالا، بر روی آبجکت Computer Management کلیک راست کرده و Connect to another Computer را زده و UNS آن مقصد را درج و OK می کنیم.

Windows Server Backup :

- در حقیقت قابلیت Backup در ویندوز Server، یک Feature است که باید نصب شود.
- یعنی در Tools وارد Add Roles and Features شده و در بخش انتخاب Feature، گزینه ی Windows Server Backup را تیک زده و نصب می کنیم.
- این قابلیت Backup در ویندوز Server، یک قابلیت local محسوب می شود.

یعنی نمی توانید Windows Server Backup را روی یک DC نصب کرده و بصورت Remote یا از طریق یک مدیریت متمرکز، اقدام به تهیه Backup از یک کامپیوتر دیگر کنید.

- این Feature باید روی هر کامپیوتری که قصد تهیه Backup از آنرا دارید نصب شود.

سیستم Windows Server Backup :

- از Tape پشتیبانی نمی کند.
- از هر درایو نوری که توسط File System قابل دسترسی نباشد، پشتیبانی نمی کند.
- فقط یک job (پروژه ی Backup) را می تواند schedule کند.
- نمی تواند یک job را طوری زمانبندی کند که بصورت یک یا n روز در میان Backup گیری کند.
- Backup گیری نوع Differential را پشتیبانی نمی کند.
- نمی تواند یک job که شامل هر دو نوع full و Incremental است را زمانبندی کند.
- فایل Backup را به فرمت VHDX ایجاد می کند که می توان آن را توسط Hyper-V یا Disk Management هم استفاده کرد.
- فقط می تواند از پارتیشن هایی Backup و Restore داشته باشد که دارای فایل سیستم NTFS هستند.
- هر دو نوع Partition Table های GPR و MBR پشتیبانی می شوند.
- همیشه از کل پارتیشن Backup می گیرد و نمی تواند از فایل ها یا فولدرهای خاصی Backup بگیرد، بجز حالت System State که فقط از اطلاعات مربوط به شبکه Backup گرفته می شود.
- بهتر است ابتدا بصورت دستی Full Backup تهیه شود.سپس Backup های incremental زمانبندی شوند.
- هنگام Restore کردن می توان فقط فایل یا پوشه ی خاصی را بازگردانی کرد.

: Windows Backup implementation

در ابتدا:

- یک سیستم با Windows Server و عضو Domain را برای این کار اختصاص می دهیم و هم نقش File Server را روی آن نصب و راه اندازی می کنیم و درایوی که جهت Backup تدارک می بینیم باید فرمت NTFS داشته باشد.
- بر روی تک تک سیستم هایی که قصد تهیه ی Backup از آنها داریم، این Role را نصب می کنیم.

```
icm DC1,Web-Server,HyperV-SRV {Install-WindowsFeature Windows-Server-Backup}
```

1. **Local Backup ها را راه اندازی می کنیم.**

وارد تک تک Server های موردنظر می شویم و به عنوان اولین Back گیری، در سمت چپ این کنسول، روی local Backup کلیک راست کرده و گزینه ی Backup once را می زنیم.

- چون از قبل هیچ Backup ای نداریم، Different Options را می زنیم.
- اگر فقط بخواهیم از AD و تمام محتویات و تنظیمات آن، نسخه ی پشتیبان بخواهیم، Custom را انتخاب می کنیم.
- گزینه ی Add Items را می زنیم. مثلاً برای پشتیبانگیری از AD، کافی ست گزینه ی System State را انتخاب کنیم.
- اگر نخواهیم از چیزی Backup گرفته شود، وارد Advanced Setting شده و با Add Exclusion آن را انتخاب می کنیم.
- وارد تب VSS می شویم.

2. **با استفاده از قابلیت VSS نیازی به بستن نرم افزارها و فایل ها برای Backup گیری نخواهد بود.**

نکته: برای backup گرفتن از SQL Server و Exchange Server که تراکنش های مداومی دارند، گزینه ی VSS copy backup را می زنیم.

- مقصد ذخیره سازی را مشخص می کنیم، که local به معنی همین سیستم جاری می باشد. اما در اینجا shared network folder انتخاب می کنیم.

اما از قبل برای هریک از Server ها، یک پوشه برای Bacup آن، در سیستم File Server ایجاد وآنها را share کنیم، و share permission را برای User یا User های مورد نظر، Full Controll تعیین کنیم. سپس آدرس UNC این پوشه را کپی و در نوار Location ، Paste می کنیم.

- اگر گزینه ی Do not inherit را انتخاب کنیم، یعنی فقط یک کاربر حق دسترسی به این Backup را دارد که باید تعیین شود.
- اگر گزینه ی inherit را بزنیم، تنها کاربرانی که در بخش Access Permission آن پوشه مجاز شده اند، دسترسی خواهند داشت.

نکته: نمی توانیم از System State بطور مستقیم توسط گزینه ی Remote، بر روی شبکه، Backup بگیریم! بایستی این نوع Backup بصورت local و بر روی Drive های محلی قرار بگیرد.

- اگر پس از پایان ویزارد، Backup شروع نشد، در کادر سمت چپ، بر روی آبجکت Local backup کلیک راست کرده و Backup once را می زنیم.

3. **Recovery را انجام می دهیم.**

- در کادر سمت چپ، بر روی آبجکت Local backup کلیک راست کرده و Recovery را می زنیم.
- چون Backup را در File Server ذخیره کرده ایم، گزینه ی دوم را انتخاب کرده و next.
- Remote shared folder را می زنیم و مسیر فایل Backup را درج می کنیم.
- پس از گذر از تاریخ، می توانیم تعیین کنیم که چه چیزی بازیابی شود.مثلاً : System State
- اگر بخواهیم Backup کاملاً صحیح و مثل اصل، بارگذاری شود، گزینه ی original location را می زنیم.
- اگر گزینه ی Perform an authoritative restore of AD Files را بزنیم، سیستم های دیگر شبکه، قادر نخواهند بود که با Backup بازگردانده شده، replicate شوند.

نکات:

- **اگر از AD نسخه ی پشتیبان تهیه کرده باشیم، فایل Backup تهیه شده، تنها 60 روز قابل بازیابی خواهد بود.**
- **برای Recover کردن Backup مربوط به AD، لازم است که سیستم AD را restart کرده و توسط فشردن دکمه ی F8 وارد حالت DSRM شویم و با حساب local admin وارد شده و به کنسول Backup رفته و آن را به صورت system state و original location (اگر بخواهیم SYSVOL هم بازیابی شود، .Perform an auth را هم فعال می کنیم.) بازیابی کنیم.**
- **اگر از drive C نسخه ی پشتیبان تهیه کردیم، نباید آن را بر روی سیستمی که درایو ویندوزش D است، recover کرد.**

Trust :

Trust را می توان نوعی توافقنامه ی امنیتی بین دو بخش از شبکه دانست.
بر اساس این توافقنامه ی امنیتی، کاربری متعلق به یکی از طرفین قرارداد، می تواند به منابعی مثل پرینترها یا فایل های **share** شده روی طرف دیگر قرارداد، دسترسی داشته باشد.

بین تمام **Domain** های یک **Tree** و نیز تمام **Tree** های یک **forest** ، بصورت پیشفرض **Trust Relationship** وجود دارد.
در یک **Trust Relationship** یک طرف قرارداد، **trusted** یا مورد اعتماد قرار گرفته، محسوب می شود و طرف دیگر، **Trusting**یا اعتماد کرده.
یعنی برای دسترسی به یک فایل **Share** شده، **Domain** یا **forest** کاربری که قصد دسترسی به فایل **share** شده را دارد، **trusted** است، و **Domain** یا **forest** ای که فایل را **share** کرده، **trusting** است.
یعنی دامین **trusting** به دامین **trusted** اعتماد کرده است!

Trust Relationship Status :

- بین دو **Domain**
- بین دو **Forest**
- بین یک **Forest** و یک **Domain** در **Forest** دیگر
- بین یک محیط **Active Directory** و یک محیط دیگر (شبکه لینوکسی): در این حالت از **Realm Trust** استفاده می شود.

Trusting: سمتی از رابطه است که اعتماد می کند و منابعش را در اختیار می گذارد.
Trusted: سمتی از رابطه که به او اعتماد شده است.

Trust Types:

- **Incoming Trust** : سمتی از رابطه که اعتماد کرده و منابعش را تحت **Trust** در اختیار گذاشته است.
- **Outgoing Trust** : سمتی از رابطه که مورد اعتماد واقع شده و برای استفاده از منابع سمت دیگر، عمل می کند.

پس بر طبق قاعده:

- ✓ **Trusting** ها، از نوع **Incoming Trust** خواهند بود.
- ✓ **Trusted** ها، از نوع **Outgoing Trust** خواهند بود.

Trust دو ویژگی مهم دارد:

1. Trust Direction:

این ویژگی نشان می دهد که کدام سیستم اعتماد کرده است، و کدام سیستم مورد اعتماد واقع شده است و دو حالت دارد:
One-way Trust
Two-way Trust

2. Trust Transitivity یا انتقالپذیریِ اعتماد :

- **Transtive یا Forest Trust :**

اگر دامین A به دامین B اعتماد داشته باشد و اگر دامین B به دامین C اعتماد داشته باشد، آنگاه دامین A نیز به C اعتماد خواهد داشت.

- **Nontransitive یا External :**

یعنی هم بین دامین های A و B اعتماد وجود داشته باشد و هم بین دامین های B و C، اما بین دامین های A و C اعتماد وجود نداشته باشد.

با تعریف Transitive Trust بین Domain A و Domain B علاوه بر اینکه این دو Domain به یکدیگر Trust می کنند، بین کلیه ی Child Domain های هردو طرف نیز رابطه ی Transitive Trust ایجاد می شود.
حال اگر در یک Transitive Trust به هر دلیلی Domain A نخواهد به یکی از Child Domain های Domain B اعتماد کند، می تواند با اعمال یک محدودیت، مانع از دسترسی آن Child Domain به منابع اش شود.

Create a Trust :

بین دو Forest :

- ✓ اولاً باید یک ارتباط فیزیکی قابل Ping بین Root Domain هر دو Forest برقرار باشد.
- ✓ هر دو Root Domain باید بتوانند همدیگر را از طریق Name هایشان نیز Ping کنند، پس نیاز به پیکربندی سرویس DNS در هردو طرف می باشد.

برای اینکه این دو Forest مختلف را از لحاظ DNS به یکدیگر مرتبط کنیم، نیاز است که درون هریک از آنها یک Stub Zone از Forest دیگر ایجاد شود.

- در Forest A وارد DNS می شویم تا یک Forward Lookup Zone از نوع Stub Zone ایجاد کنیم.
- پس با کلیک راست بر روی Forward Lookup Zone گزینه ی New Zone را و سپس Stub Zone و سپس گزینه ی To all DNS...in this Forest را می زنیم.
- برای Zone Name باید نام Forest B و یا Zone ای که بر روی Forest B قرار دارد را وارد کنیم ، مثلاً : payamavar.local
- برای Master Servers، آدرس IP مربوط به Forest B را وارد کرده و گزینه ی ..Use the above Servers to cre را فعال می کنیم.
- حال باید Zone Transfer را هم فعال کنیم، پس وارد Properties گزینه ی مربوط به خود Forest Name می شویم.
- در تب Zone Transfers گزینه ی Allow Zone transfer را فعال کرده و only to following Servers را زده و Edit.
- IP مربوط به Forest B را وارد کرده و همه ی تب ها را OK و خارج می شویم.
- دقیقاً همین کارها را در Forest B انجام می دهیم اما با Zone Name مربوط به Forest A .

- برای تست DNS Configuration باید بتوان در هریک از Root Domain ها به آدرس main Domain دیگری Ping کرد.

- در Forest A وارد کنسول Active Directory Domains and Trusts می شویم.
- در کادر سمت چپ، وارد Properties گزینه Forest A می شویم و تب Trust را انتخاب می کنیم.
- **نکته:** همانطور که می بینید، اگر Child Domain در شبکه وجود داشته باشد، از قبل بطورخودکار با آن یک Trust ایجاد شده است!
- گزینه ی New Trust را زده و نام Forest مقصد را وارد می کنیم و Next.

سپس nontransitive و یا transitiv بودنِ ارتباط را مشخص می کنیم.

سپس پرسیده می شود که آیا این Trust فقط روی این Domain ایجاد شود یا هم اینجا و هم بر روی Domain مقابل نصب شود؟

با فرض اینکه Both را انتخاب کرده باشیم، پس نیاز است که مشخصات یک Administrator User از طرف مقابل را داشته باشیم و وارد کنیم.

- ○ Forest-Wide Authentication : تمام User های هر طرف، قادر به authenticate کردن و برقراری ارتباط با یکدیگر هستند.
- ○ Selective Authentication : باید خودمان تعیین کنیم که کدام User ها مجاز به authentication باشند.

- حال برای outgoing Trust هم یکی از دو گزینه ی بالا را انتخاب و Next!
- سپس باید این Trust ها confirm کنیم و تمام!

نکته: فرض کنید که در هنگام ایجاد Trust آن را روی Forest-wide قرار داده بودیم، حال که آن را نصب کرده ایم، قصد تغییر آن را داریم، پس دوباره وارد تب Trust شده و Trust مورد نظر را در هریک از کادرها انتخاب کرده و properties و سپس در تب Authentication!

نکته: پس از ایجاد یک Trust بین دو Forest ، به سادگی می توان در هریک از Forest ها یک Domain Local Group ایجاد کرد و در تب members آن، Userهایی را از Forest دیگر به عضویت در آورد.

Web Server :

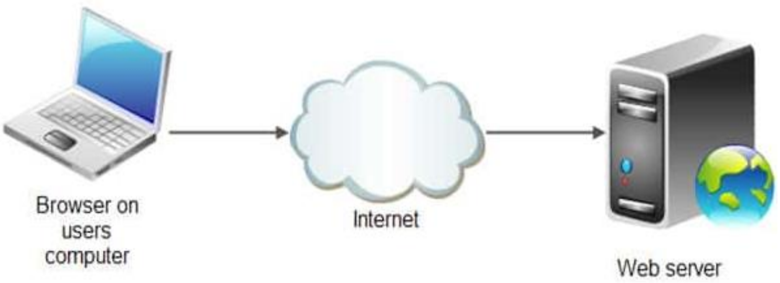
- از جنبه ی سخت افزاری، **Web Server** یک رایانه است که نرم افزار **Web Server** و فایل های اجزای یک **Website** را ذخیره می کند، شامل: فایل های **HTML**، تصاویر، فایل های جاوا اسکریپت و ... .
- **Web Server** باید متصل به اینترنت باشد.
- از جنبه ی نرم افزاری، یک **Web Server** شامل چندین بخش (حداقل یک سرور **HTTP**) است که چگونگی دسترسی کاربران به فایل های روی **Host** را کنترل می کند.

- **Website** هایی که در **Web Server** ذخیره می شوند، از طریق نامِ **Domain** ای آن، قابل دسترس می باشند و محتوای آن به دستگاه کاربر نهایی عرضه می شود.

برخی از نرم افزارهای مورد استفاده به عنوان **Web Server** :

- **Apache** (Apache HTTP Server)
- **GWS** (Google Web Server)
- **Nginx**
- **Lighttpd**
- اما نسخه ی **Microsoft** برای آن، **IIS** (Internet Information Services) می باشد که به شکل یک **Role** در خود **Windows Server** قابل نصب و راه اندازی است.

در حقیقت **Web Server** یک برنامه ی کامپیوتری است که صفحه های وب درخواست شده در شبکه را، کنار هم قرار می دهد.
اما در شکل کلی **Web Server** سامانه ای است که توانایی پاسخگویی به یک مرورگر وب و ارسال صفحه ی درخواستی **Browser** را داراست.



وقتی شما پشت کامپیوتر خود نشسته اید، اولین کاری که برای دیدن یک سایت در اینترنت انجام می دهید، وارد نمودن آدرس آن سایت در مرورگر خود می باشد.

- درخواست شما وارد محیط اینترنت شده و به سوی **Web Server** مربوط به آن وبسایت فرستاده می شود.
- صفحات وب بر پایه ی یک ساختار مشخص و با **IP** مشخص، بر روی **Web Server**، که او هم یک **IP** مشخص دارد، قرار می گیرند.

- وقتی کسی قصد برپایی یک وبسایت داشته باشد، نیاز به یک **Web Server** برای متصل کردن وبسایتش به آن را خواهد داشت.
یعنی اول فایل های وبسایت را در یک سیستم **Host** آپلود می کنیم و یک **Link** دریافت می کنیم.
سپس ساختار طراحی شده ی وبسایت را در یک **Web Server** آپلود و پیکربندی می کنیم و برای استفاده از فایل های روی **HOST** از لینک دریافت شده استفاده می کنیم.
حال هرکسی که آدرس وبسایت را در مرورگر وارد کند، درخواستش به **Web Server** شما می رسد.
- نکته اینجاست که **Host** می تواند مثل یک رسانه ی ذخیره سازی، مثل یک **Hard Disk** در سیستم **Server** قرار گرفته باشد.
یعنی **Web Server** و **HOST** می توانند هردو تحت یک سیستم کار کنند.

- مرورگرها، تنها با زبان های HTML و CSS کار می کنند؛ و مثلاً PHP و ASP.net ... را متوجه نمی شوند.
- WEB SERVER به درخواست های کاربران بر روی شبکه گوش داده و آنها را با ابزار Web Browser پاسخ می دهد.
- Web Browser با سرویس WWW کار می کند.
- هر کامپیوتری می تواند با نصب نرم افزار Web Browser، به یک دستگاه Web Server (خدمات رسان وب) تبدیل شود. اما با توجه به بالا بودن هزینه‌های قطعات سخت افزاری نیرومند، نیروی پشتیبانی و ....، راه اندازی یک Web Host و Web Server در کنار هم، به صرفه نیست.
- پس شرکتهایی این مسئولیت را پذیرفته و بخشی از فضای ذخیره سازی سرورهای خود را به صورت اجاره‌ای در اختیار متقاضیان قرار می‌دهند.
- به این شرکتهای ارائه کننده‌ی خدمات میزبانی‌وب، Hosting می‌گویند.

در حالت کلی Web Browser ها دارای ویژگی های زیر می باشند:

- Authentication : قبل از اینکه اجازه ی دسترسی به درخواستِ کاربر را بدهد، آن را شناسایی می کند.
- Access Permission : اجازه ی دسترسی به منابع را به کاربر می دهد.
  (مانند محتویات فایل ها که بر روی File Server وجود دارد).
- ساختار Dynamic : که با یک یا تعدادی از تکنولوژی های SI ، GI ، CGI ، FastCGI ، JSP ، PHP ، ASP ، ASP.NET پیاده سازی می شود.

یک سیستم Web Host باید حداقل امکانات زیر را داشته باشد:

- اتصال دائم و پر سرعت به اینترنت.
- از نظر سخت افزار و قطعات داخلی باید قدرتمند بوده تا امکان پاسخگویی به درخواست مراجعه کنندگان را داشته باشد.
- نرم‌افزارهای لازم برای اجرای انواع فایلها از لحاظ نوع برنامه نویسی را داشته باشد.
- نرم‌افزارهای مورد نیاز برای مدیریت بخشهای مختلف سایت و پست الکترونیک و ... را در اختیار مالکان و مدیران وبسایت ها قرار دهد.

IIS:

- این Web Server را شرکت Microsoft ارائه نموده است.
- در واقع IIS مجموعه ای از سرویس های اینترنتی است که به صورت یکجا نمایش داده می شوند.
- بعد از Apache، بیشترین محبوبیت را بین کاربران دارد.
- وب سرور IIS تنها در ساختار Microsoft Windows قابل ارائه می باشد و در Platform های دیگر مثل Linux قابل راه اندازی نیست.

Local Host :

فرض کنید که یک **Web Programmer** هستید و نیاز دارید که تمامی تست های خود را که ممکن است باعث اختلال در کار نیز بشوند را انجام دهید.
منطقی نیست که نرم افزار را با صرف هزینه ای برای خرید یک **Web Host** در اینترنت قرار دهید، از طرف دیگر ممکن است نرم افزار شما دارای
Bug های امنیتی باشد که بعد از قرار دادن در اینترنت ممکن است هک شود.
در این حالت بهتر است که نرم افزار را در سیستم خود اجرا کنید و پس از انجام آزمایش ها و تست ها، در نهایت در یک **Web host** اینترنتی قرار دهید.
برای اینکار باید یک **Host** مجازی بر روی سیستم خود ایجاد کنید که به آن، **Local Host** گفته می شود.

برای ایجاد یک **Local Host** نیاز به نصب و راه اندازی گزینه های زیر می باشد:

- **Web Server Software** : مثل IIS و …
- **Web Programming Language** : مثل PHP، Java Script و …
- **Mail Server** :
- **FTP Server** :

می توان تک تک این گزینه ها را روی سیستم نصب کرد.
و یا می توان از نرم افزارهای آماده ای که شامل تمامی این گزینه ها هستند، استفاده نمود:

- **Wamp** : برای Windows
- **Lamp** : برای Linux
- **Xampp** : برای همه ی OS ها

IIS Implementation :

حداقل به دو Server نیاز داریم:

- ❖ DC : شامل نقش های Domain Controller و DNS: آنها را به شکل معمول راه اندازی می کنیم.
- ❖ Web Server : شامل نقش IIS: بطورکلی جهت نصب این Server از دستور زیر می توان آن را فوری انجام داد:

```
Install-WindowsFeature -Name web-server ,web-mgmt-service
```

اما اگر قصد تنظیمات جزیی تری جهت راه اندازی یک WebSite را داشته باشیم، به شکل زیر از طریق GUI پیش می رویم:
توسط Add Roles and Features وارد شده و هنگام نصب این Role، نقش Web Server (IIS) را انتخاب می کنیم.
در تب Select Role services، گزینه های زیر را می توان فعال کرد:

- Default Document: قابلیت راه اندازی صفحه ی پیشفرض برای تمامی صفحات وبسایت خواهد بود.
- Directrory Browsing: در صورتی که صفحه ی مربوط به یک link تنظیم نشده باشد، محتویات موجود در وب سرور را نشان می دهد (لیست می کند).
- HTTP Errors: توسط این قابلیت، درخواست هایی از وبسایت، که در وبسایت وجود نداشته باشند یا قابل دسترسی نباشند را به صفحات پیشفرضی برای آن طراحی شده اند (مثلاً این صفحه حذف شده است / این صفحه موجود نیست)، هدایت می کند.
- Static content: جهت نمایش محتویات ثابت در وبسایت کاربرد خواهد داشت.
- Http Redirection: توسط این قابلیت می توان درخواست های کاربران را به یک آدرس دیگر، ارسال یا redirect کرد.
- توسط زیرگزینه های Heakth and Diagnostics می توان سلامت و ایرادهای وبسایت را زیرنظر داشت.
- توسط گزینه های Performance می توان قابلیت فشرده سازی را جهت داده های درخواستی کاربران فعال کرد. که البته این قابلیت یک عیب هم دارد، که این است که سرعت تبادل داده با کاربر را کاهش می دهد.
- توسط زیرگزینه های Security می توان امنیت وبسایت را افزایش داد. مثلاً توسط گزینه ی IP and domain Restric.. می توان تعیین کرد که کاربران با کدام رنج آدرس IP بتوان از سایت دیدن کنند و یا فایلی دانلود کنند و ... .
- توسط گزینه های FTP Server می توان تبادلات داده توسط این پروتکل را نیز فعال کرد.

درحقیقت می توان همه ی گزینه ها را نیز فعال کرد، هرچند که همه ی آنها به کار ما نخواهند آمد، مثل:

- ○ Application Development
- ○ IIS 6 Management Compa ...
- ○ IIS Management Scripts and Tools
- ○ Management Service

- ▪ پس از نصب، در پنجره ی Server Manager گزینه ی IIS را مشاهده خواهید کرد که نشان می دهد بر روی کدام Server نصب شده است.
- ▪ از قسمت Tools می توانیم از طریق گزینه ی Internet Information Services Manager وارد کنسول آن شویم.
- ▪ بطور پیشفرض یک وبسایت به نام Default Web Site ایجاد کرده و یک صفحه ی web برای آن می سازد، به نام iisstart.htm که می توان آنها را از کادر چپ و در زیرگزینه های آبجکت Server مشاهده کرد.
- ▪ درحقیقت در هر IIS Server می توان بیش از یک Website را راه اندازی کرد، که همه ی آنها را در همین کادر سمت چپ و زیر گزینه ی Sites مشاهده خواهیم کرد.
- ▪ از این به بعد، اگر در هریک از سیستم های متصل به شبکه یا در خود این Server، وارد مرورگر شده و آدرس IP خود Web Server را و یا عبارت localhost را درج کنیم، صفحه ی iisstart باز خواهد شد.

- ❖ برای اطمینان از اینکه در یک سیستم، سرویس IIS نصب و فعال است یا خیر، در PowerShell درج می کنیم:

```
Get-Service w3svc
```

و باید در حالت Running قرار داشته باشد.

:Implement a Website

- در ابتدا فایل های **Source** وبسایت را در پوشه ای در خود سیستم ذخیره می کنیم.
- در همان کنسول **IIS** و در کادر سمت چپ، بر روی آبجکت **Sites** کلیک راست کرده و **Add Website** را می زنیم.
- برای نواز **Site name**، نام وبسایت را همراه با نام **Domain** اش، درج می کنیم، مثلاً: **payamavar.de**
- برای **Physical path**، آدرس پوشه ای را که فایل های **source** وبسایت در آن قرار دارند، انتخاب می کنیم.
- برای اولین بار، **Type** را بر روی **http** و **Port** را **80** درج می کنیم.
- برای **IP address**، آدرس **IP** مربوط به خود **Web Server** را انتخاب یا درج کرده و **OK** می کنیم.

حال می توان تنظیمات متفرقه ی وبسایت را انجام داد؛ پس ابتدا در کادر سمت چپ، آبجکت آن را انتخاب می کنیم، و در روبرو:

- با دابل کلیک، وارد **Default Document** می شویم.
- درحقیقت یا می توان یکی از صفحات وبسایت را برای اینکار درنظر گرفت و یا یک صفحه را جهت ارجاع به عنوان صفحه ی پیشفرض وبسایت، ایجاد کرد. مثلاً در اینجا صفحه ی اول و اصلی وبسایت یا همان **Home** را در نظر می گیرم.
- در کادر سمت راست، روی **Add** کلیک کرده و برای **Name** درج می کنیم: **home.html**

- **DNS Server** را تنظیم می کنیم:
  - وارد کنسول **DNS** و **forward lookup zone** مربوط به **payamavar.de** می شویم.
  - یک **A Record** ایجاد کرده و نام آن را www و **IP** مربوط به payamavar.de را برای آن درج می کنیم و **OK**.

:Secure a Website

درحقیقت هر تبادل داده ای که توسط مرورگرهای Web انجام شود، توسط پروتکل http خواهد بود.

اما یکی از ضروری ترین کارها جهت امن کردن Web Server، استفاده از پروتکل https می باشد.

- **HTTPS همان HTTP است که S، مخفف Secure است! به این معنی که پروتکل HTTP ای که توسط SSL، امن شده است.**
- **پروتکل SSL از Certificate ها جهت تضمین امنیت استفاده می کند.**
- **نمی توان جهت انتقال فایل های بسیار بزرگ، از آن استفاده کرد.**
- **جهت ارسال و دریافت ایمیل توسط Web mail ها نیز کارآیی دارد.**
- **http از پورت 80 استفاده می کند.**
- **https از پورت 443 استفاده می کند.**

به این شکل که:

- ارتباط میان Web Server با Domain Controller بر اساس پروتکل https شکل بگیرد.
- ارتباط میان Web Server با تمامی Client ها نیز بر اساس پروتکل https انجام بگیرد.

تا تمامی تبادلات داده ای با Web Server، رمزنگاری شده باشند.

جهت تدارک دیدن SSL Certificate، به سه روش می توان عمل کرد:

- ❖ **صدور Certificate بصورت self-signed، که توسط خود کنسول IIS ایجاد می شود:**
  - **در کنسول IIS، در کادر سمت چپ، آبجکت خود Server را انتخاب کرده و در کادر میانی، وارد Server Certificates می شویم.**
  - **از طریق گزینه ی Create Self-signed Certificate در کادر سمت راست، می توان پیش رفت.**
- ❖ **راه اندازی یک CA Server در شبکه و دریافت این SSL Certificate از آن:**
  - **در ابتدا نیاز است که در شبکه مان، یک CA Server راه اندازی کرده باشیم.**
  - **سپس در IIS Server (Web Server)، یک درخواست SSL Certificate را به CA Server ارسال می کنیم؛ پس در کنسول IIS، در کادر سمت چپ، آبجکت خود Server را انتخاب کرده و در کادر میانی، وارد Server Certificates می شویم.**
  - **در کادر سمت راست، وارد Create Domain Certificate می شویم.**
  - **برای Common name نام کامل وبسایت را درج می کنیم: www.payamavar.de**
  - **برای Organization نام دامینی که در آن Web Server را نصب کرده ایم را وارد می کنیم: payamavar0**
  - **گزینه های دیگر را به دلخواه وارد می کنیم.**
  - **برای Online Certification Authority گزینه ی Select را زده و CA Server را انتخاب می کنیم.**
  - **برای friendly name هم دوباره آدرس کامل وبسایت را درج می کنیم: www.payamavar.de و finish.**
  - **پس از چند لحظه، باید در کادر میانی یک Certificate با مشخصات، در یک سطر ظاهر شوند.**
- ❖ **خریدن یک SSL Certificate از شرکت های معتبر:**
  - **درحقیقت فقط برای وبسایت های سازمانی و یا برای وبسایت های آزمایشی، و هر وبسایتی که به اینترنت متصل نخواهد شد، می توان از CA Server و یا از IIS-Self-Signed Certificate استفاده کرد، که هم هزینه ی اضافی را در بر نخواهد داشت و هم کفایت کرده و امنیت را پشتیبانی می کند.**

حال که Certificate را برای وبسایت موردنظر، صادر و وارد کردیم، می توانیم http را برای وبسایت، به https تغییر دهیم، پس به آبجکت Site رفته و آبجکت آن وبسایت را انتخاب کرده و در کادر سمت راست، وارد Bindings شده و یکبار Add را می زنیم.

Type را بر روی https و Port را روی 443 قرار داده و آدرس IP موردنظر را وارد کرده و توسط منوی SSL certificate، گواهی import شده برای آن را، انتخاب کرده و OK.

:Publish a Website

درحقیقت، منتشر کردن یک وبسایت، یعنی هرکاربری در محیط اینترنت، قادر به فراخوانی وبسایت ما، توسط پروتکل **http** یا **https** باشد.

- از آنجایی که یک **Web Server** ایمن و قدرتمند، دارای یک **Firewall** یا **Firewall server** قدرتمند هم خواهد بود، اولین قدم این است که پورتهای مربوط به **http** و **https** و **FTP** را بر روی **firewall**، باز کنیم، که اجازه ی عبور و مرور داده ای داشته باشند.

AD CS (Active Directory Certificate Services) :

PKI:

درحقیقت نوعی رمزنگاری قدرتمند وجود دارد به نام **PKI** (Public Key Infrastructure) یا رمزنگاری کلید عمومی، که تحت آن، نوعی مجوز دسترسی به نام گواهینامه یا **Certificate** را جهت امنیتِ دسترسی ها، تولید و مدیریت می کنیم.

Certificate مثل اثر انگشت الکترونیکی است که از یک کلید عمومی به نام **PKI** (**Public Key Infrastructure**) استفاده می کند تا بتواند بیشترین سطح امنیت را فراهم کند.

هر گواهینامه یا **Certificate** ، وظایف و کارهای مشخصی انجام می دهد:

- ✓ بعضی از **Certificate** ها برای **encryption** و **decryption** به کار می روند.
- ✓ بعضی از آنها برای **Authentication** ها بکار می روند.
- ✓ بعضی از آنها برای سرویس خاصی کاربرد دارند.

بطورکلی وظایف هر **Certificate** درون خود **Certificate** تعبیه شده اند.

- ○ مثلاً برای راه اندازی پروتکل **SSL** جهت امن کردن وبسایت، نیاز به **Certificate** خواهیم داشت.
- ○ برخی نرم افزارها بطورمستقیم با **Certificate** کار می کنند، مثل: **Skype** و **Microsoft Exchange** و ... .

پس بسیاری از **App** ها و **Service** ها و **Role** ها، به گواهینامه یا **Certificate** ها برای عملکرد صحیح نیازمند هستند تا بتوانند به **Ressource** ها دسترسی یافته و اجرا شوند.

موسسه یا **Server** ای که **Certificate** را ارائه می دهد، **Certificate Authority** نام دارد که به **Certification** هایی که در تمام دنیا معتبر هستند، **External Certification** گفته می شود.
مثلاً موقع اتصال به سایت های اینترنتی مثل **Facebook**، این **Certificate** از طریق پروتکل **HTTPS** فعال می شود.

مزایای صدور گواهی نامه ها:

- پشتیبانی از **logon** کردن توسط **Smart Card**
- رمزگذاری ترافیک شبکه توسط **IPSec**
- رمزگذاری ترافیک وب با استفاده از پروتکل **SSL (Secure Sockets Layer)**
- رمزگذاری **File** ها و **Folder** ها با استفاده از **EFS (Encrypting File System)**

روش کار به این شکل است که ابتدا امضا کننده (**Signer**)، توسط الگوریتم **Hash**، سند را **Encrypt** می کند، سپس آن را با **private key** که فقط خودش دارد، قفل می کند و آن را روی اینترنت ارسال می کند.

نکته: در حقیقت **Private Key** مثل شناسنامه می ماند که همیشه باید دست صاحبِ آن باشد، و **Public Key** مثل کپی شناسنامه است که می توان آن را به اداره ها و سازمان ها داد!
Public Key، هم درون **CA Server** قرار دارد و هم درون هریک از **Client** ها.

Registration Authority: مرکزی یا سیستمی است که درخواست Certificate را دریافت می کند.
در حقیقت درخواست کاربران برای گواهینامه دیجیتالی را بررسی و تحویل CA Server می دهد و به او می گوید که گواهینامه دیجیتالی مناسب را برای آن کاربر ارسال کند.

Certificate Life Cycle (CLC):
هر Certificate ای که توسط CA ایجاد می شود، دارای یک مدت اعتبار (تاریخ انقضاء) است که از یک روز و ساعت معین شروع شده و در یک روز و ساعت معین باطل می شود و به صورت زیر مشخص می شود:

- Not before: month/day/year, 00:00:00 Am/Pm
- Not after: month/day/year, 00:00:00 Am/Pm

- **گواهی ها نمی توانند تمدید شوند، پس باید باطل (Revoke) شوند.**
- **برای باطل کردن یک گواهی، نیازی نیست که حتما نامعتبر و منقضی شده باشد، بلکه می توان یک گواهی تازه و فعال را هم باطل کرد.**

Certificate Revocation List (CRL) **یا لیست مدارک فسخ شده:**
باطل کردن Certificate، یعنی در صورت معتبر بودن آن، اعتبارش را از دست بدهد و در لیستی به نام CRL ثبت شود، تا سیستم، گواهی های باطل شده را بداند.

- **اگر یک گواهی را delete کنیم، هنوز هم فعال و معتبر است، چون برای غیرفعال و نامعتبر کردن آن، باید ابتدا باطلش کنیم(revoke).**
- **کارت های بانکی نیز دقیقا به همین دلیل دارای یک مدت اعتبار چند ساله هستند، چون در حقیقت خود کارت بانکی، یک Certificate است که تاریخ اعتبار دارد.**

برای مشاهده ی Certificate هایی که بر روی یک سیستم:

- **فقط برای User جاری ثبت شده اند:**
  در نوار جستجوی ویندوز، عبارت"**certmgr.msc**" را جستجو و باز می کنیم.

- **فقط برای Computer جاری** (به عبارتی برای همه ی User های روی سیستم) **ثبت شده اند:**
  - روش اول: در نوار جستجوی ویندوز، عبارت"manage computer certificates" را جستجو و باز می کنیم.
  - روش دوم: در نوار جستجوی ویندوز، عبارت"**certmgr**" را جستجو و باز می کنیم.

نکته: البته همچنین می توان به سادگی ابتدا کنسول MMC را باز کرده و توسط گزینه ی Add or Remove Snap-ins، آبجکت Certificates را اضافه کرده و نوع آن را نیز (User و یا Computer) مشخص کرده و تمام!

در پوشه ی Personal و در Certificates، گواهی های Private ثبت می شوند.
در پوشه ی Trusted Root Certifications Authorities، گواهی های Public ثبت می شوند.

:AD CS

در بسیاری از محیط های آزمایشی و محیط های داخل سازمانی، خرید Certificate از Authority های بین المللی به دلیل هزینه ای که در بر دارد، منطقی نیست. به همین دلیل در Windows Server این امکان وجود دارد که Certificate های غیربین المللی را ایجاد و استفاده کنیم.

پس در حقیقت، تحت AD CS، می توان از PKI بهره برد، یا بهتر است بگوییم، AD CS از PKI بهره می برد.

به گواهینامه هایی که از AD CS ایجاد می شوند، Self-Signed Certificate گفته می شود، که اعتبار بین المللی ندارند و فقط جهت برقراری امنیت داخل سازمانها استفاده می شوند و به آنها internal Certification گفته می شود.

پس سرویس Active Directory Certificate Services باید توسط مدیران شبکه نصب و پیکربندی و مدیریت شود تا بتوان زیرساختی برای ارائه ی Certificate ها در شبکه ی سازمان، ایجاد کرد.

قبل از اینکه Certificate منقضی شود و اعتماد آن از بین برود، باید سیستم صاحبِ آن، یک Certificate جدید درخواست دهد.

Certificate Enrollment: به اختصاص دادن یک Certificate به یک سرویس، کاربر یا کامپیوتر گفته می شود.

به سیستمی که Certificate های شبکه را صادر می کند، CA یا Certificate Authority گفته می شود.

نکته: هر CA ای نمی تواند برای یک Client خاص، گواهی صادر کند. پیشنیاز آن، وجود Trust میان CA و آن Client می باشد.

CA به دو شکل قابل راه اندازی است:

- **Enterprise CA**:
  - فقط مخصوص شبکه های Domain است.
  - همه ی Client های Domain، بطورخودکار به سیستم CA، اعتماد یا trust خواهند داشت.
  - جهت تولید Certificate می توان از Template های موجود در کنسول AD CS استفاده کرد.
  - لیست CRL در Active Directory ذخیره شده و برای همه ی Client ها قابل دسترسی خواهد بود.
- **Stand-alone CA**:
  - هم در شبکه های Work Group و هم در شبکه های Domain قابل راه اندازی است.
  - وقتی یک Client درخواست Certificate را به این CA ارسال می کند، این درخواست در CA وارد لیستی می شود، به نام Pending Request که برای تایید شدن این درخواست، مدیر شبکه باید به صورت دستی آن را در کنسول CA تایید کند.
  - جهت تولید Certificate نمی توان از Template های موجود در کنسول AD CS استفاده کرد، بلکه باید همه چیز بصورت دستی انجام گیرد. هرچند بخشی هم به نام Template Certificate وجود نخواهد داشت.

AD CS دارای شش قابلیت می باشد، که در هنگام نصب AD CS می توان به دلخواه آنها را نیز فعال و نصب کرد:

1. **CA یا Certification Authority**:
   - جهت صادر و مدیریت کردن Certificate ها به آن نیاز خواهیم داشت.
2. **Certification Authority Web Enrollment**:
   - درحقیقت Client ها به چندین روش می توانند با CA ارتباط برقرار کرده و Certificate درخواست و دریافت کنند.
   - یکی از این روش ها، Web base و توسط پروتکل HTTP یا HTTPS می باشد.
   - جهت این قابلیت، به CA Web Enrollment نیاز خواهیم داشت.
   - تحت این قابلیت، Client ها بصورت Web base می توانند:
     - یک Certificate درخواست کنند.
     - Certificate ای که صادر شده است را دریافت (download) کنند.
     - CRL را دریافت کنند. این لیست مهم است، به این جهت که اگر یک Client درخواست ارتباط با آنها را داشت، Certificate آن را بررسی کنند و ببینند که آیا جزو revoked Certificate است یا نه؛ که اگر باشد، از ارتباط جلوگیری کنند.
3. **Network Device Enrollment Service**:
   - این قابلیت جهت اختصاص Certificate به دستگاه های غیر کامپیوتر در شبکه به کار می رود، مثل Router یا Switch و ... .
   - پس این دستگاه ها توسط پروتکلی به نام Simple Certificate Enrollment Protocol (SCEP) به CA متصل شده و درخواست Certificate داده و در صورت صدور، آن را دریافت می کنند.
4. **Online Responder**:
   - یک رابط میان CA Server و تمام Client ها می باشد.
   - این قابلیت جهت بهبود و افزایش سرعت عملکرد ارتباط با CRL استفاده می شود.
   - به این صورت کار می کند که وقتی یک Client یک Certificate دریافت می کند، جهت ارتباط با CRL و استعلام وضعیت اعتبار آن Certificate، از Online Responder درخواست استعلام این اعتبار را می کند.
   - Online Responder درخواست Client را به CRL ارسال کرده و با او مکاتبه کرده و پاسخ را به Client بر می گرداند.
   - Online Responder با پروتکل OCSP (Online Certificate Status Protocol) کار می کند.
5. **Certificate Enrollment Web Service**:
6. **Certificate Enrollment Policy Web Service**:

: AD CS Implementation

برای نصب نقش AD CS وارد Add Roles and Features شده و نقش AD CS را انتخاب و در تب Role Services، گزینه ی مورد نظر را انتخاب کرده و تا پایان پیش می رویم.
در شبکه های کوچک، انتخاب فقط همان Certification Authority کفایت می کند، وگرنه که گزینه ی Certification Authority Web Enrollment را نیز فعال می کنیم.
پس از اتمام نصب، روی ..Configure Active Directory Cer کلیک می کنیم.

- در تب Credentials، باید User ای که با آن قصد تنظیم این Role را داریم، انتخاب کنیم.
- اگر قصد استفاده از AD CS بر روی سیستمی که هیچ DC روی آن نصب نیست داشته باشیم، این User باید Administrator باشد.
- اگر قصد استفاده از AD CS بر روی سیستمی که دارای AD است داشته باشیم، این User باید جزو گروه Enterprise Admins باشد.

- Certification Authority را انتخاب می کنیم.
- اگر دارای یک Active Directory بر روی سیستم باشیم اما قصد داشته باشیم که سرویس Certification Services را بدون اتصال به Active Directory، و بصورت Offline نصب کنیم، پس Standalone CA را انتخاب می کنیم، درغیر اینصورت Enterprise CA را و اگر که این سیستم، جزئی از Domain نباشد، اصلا گزینه ی Enterprise خاموش خواهد بود.
- اگر برای اولین بار است که CS را راه اندازی می کنیم، باید Root CA را انتخاب کنیم.
- از آنجایی که هر AD CS دارای یک Private Key است، باید برای آن یکی تعیین کنیم، پس اگر برای اولین بار است، گزینه ی Create a new را می زنیم.

- نوع Cryptographic Provider را روی Microsoft Software Key Storage Provider قرار داده و نوع Hash را نیز بصورت Default رها می کنیم.
- یک نام و یک آدرس distinguished برای این CA ایجاد می شود.
- در ادامه باید تاریخ انقضای این CA را تعیین کنیم، پس با توجه به تاریخ انقضایی که قرار است در آینده برای Certificate ها تعیین کنیم، این تاریخ را تعیین می کنیم.

نکته: معمولا برای امنیت بیشتر، Root CA را بصورت Standalone CA پیکربندی می کنند و چند Server دیگر را به عنوان Subordinate CA تنظیم می کنند.
و از طرفی، وقتی درخواست صدور گواهینامه، برای Standalone CA ارسال می شود، باید تمام اطلاعات و هویت درخواست کننده در درخواست ذکر شده باشد. چون این نوع CA مثل Enterprise CA نیست که بتواند اطلاعات کاربران و کامپیوترها را از AD استخراج کند.

قابلیت	Enterprise Root CA	Standalone Root CA
حضور در اکتیودایرکتوری و استفاده از امکانات آن	بله	خیر
میتواند آفلاین باشد؟	ترجیحا خیر	ترجیحا بله
اختصاص خودکار گواهی ها	بله	بله ولی توصیه نمیشود
صدور گواهی ها توسط ادمین بصورت دستی	بله	بله
صدور گواهی نامه ها بصورت خودکار	بله	خیر
استفاده از Template ها	بله	خیر
احرازهویت درخواست کننده گواهی از طریق AD DS	بله	خیر

حال وقتی وارد کنسول **Certification Authority** شویم، در زیر مجموعه ی گزینه ی **Root CA**، پوشه های زیر را می بینیم:

- **Revoked Certificates** : لیست **Certificate** های باطل یا **expire** شده را می بینیم.
- **Issued Certificates** : لیست **Certificate** های صادر شده را می بینیم.
- **Pending Requests** : لیست **Certificate** های درخواست شده را می بینیم که باید تایید یا رد شوند.
- **Failed Requests** : لیست **Certificate** هایی که به دلیل مشکلاتی که دارند، با شکست مواجه شدند.
- **Certificate Templates**: می دانیم که این پوشه تنها در **Enterprise CA** ها موجود است و شامل یک سری گواهی های نمونه ی آماده می باشد که می توان با کمی تغییر در هریک، همان را دوباره صادر و استفاده کرد.

و در صورت نیاز به یک گواهی جدید، روی همین پوشه کلیک راست کرده و **New** و **Certificate Template to Issue** را می زنیم.

می دانیم که درخواست های دریافت **Certificate** به **CA** ارسال خواهند شد، و دو حالت وجود دارد، یا اینکه بطورخودکار رسیدگی شوند، و یا اینکه به پوشه ی **Pending Request** رفته و منتظر تایید ما باشند.

- ❖ حال برای اینکه این دو حالت را مشاهده یا تنظیم کنیم، روی آبجکت **CA Server** در کادر سمت راست کلیک راست کرده و به **Properties** و تب **Policy module** رفته و دکمه ی **Properties** می رویم.
  - گزینه ی اول (**set .. to pending**) درخواست ها را به پوشه ی **pending** ارسال کرده و منتظر **approval** ما می مانند.
    در **Stand alone CA** بطور پیشفرض این گزینه فعال است.
  - گزینه ی دوم (**follow ... template**) آنها را بطورخودکار و با توجه به **template** های ما، تایید یا تنظیم می کند.
    در **Enterprise CA** بطور پیشفرض این گزینه فعال است.

- ❖ برای اینکه **CRL** را جهت دسترسی **Client** ها تنظیم کنیم که بتوانند آن را دریافت و روی خودشان ثبت کنند، دوباره وارد **Properties** آبجکت **CA Server** در سمت راست شده و به تب **Extensions** می رویم.

:Client Certificates

- برای مشاهده ی Certificate های موجود بر روی یک کامپیوتر:

Cmd را با دسترسی مدیر باز می کنیم و وارد می کنیم: mmc
Add or Remove Snap-ins را باز کرده و از سمت چپ، گزینه ی Certificates را به شکل Computer account اضافه و باز می کنیم. در کادر سمت چپ، وارد شده و پوشه ی Personal و پوشه ی Certificates را باز می کنیم که Private Certificate ها قرار خواهند داشت. اما در پوشه ی Trusted Root Certifications Authorities گواهی Public، مربوط به CA Server ای که Client جاری به آن Trust دارد را مشاهده خواهیم کرد.
پس برای اینکه یک Client به یک CA Server اعتماد داشته باشد، باید Public Certificate را در این پوشه import کنیم، که معمولاً در شبکه های work group با این مساله روبرو خواهیم بود.

- برای درخواست Certificate:

Client ها به سه روش می توانند، درخواست Certificate را به CA ارسال کنند.

1. MMC (Microsoft Management Consol):

- Cmd را با دسترسی مدیر، باز می کنیم و وارد می کنیم: mmc
- Add or Remove Snap-ins را باز کرده و از سمت چپ، گزینه ی Certificates را به شکل Computer account اضافه و باز
- می کنیم. در کادر سمت چپ، وارد شده و پوشه ی Personal را نیز باز کرده و کلیک راست کرده و All tasks و سپس
- Request New Certificate را می زنیم.
- Active directory Enrollment Policy را انتخاب می کنیم.
- نسخه ی Computer را انتخاب کرده و Enroll را می زنیم.
- در صورتی که در مقابل گزینه ی STATUS، کلمه ی Succeeded درج شده باشد، به معنای ارسال موفقیت آمیز این درخواست به CA Server می باشد.
- پس اگر در همان کنسول MMC و پوشه ی Personal نگاه کنیم، می بینیم که Certificate ایجاد شده است.

2. Web Base (HTTP/S):

- وارد یک Web Browser شده و در address bar آدرس IP و یا FQDN مربوط به CA Server را به صورت زیر وارد می کنیم:
http://myCA.payamavar.local/certsrv
- یک credential مدیریتی وارد می کنیم.
- می بینیم که از نام هریک از گزینه ها، عملکردش پیداست. بر روی Request a certificate کلیک می کنیم.
- Advanced certificate request را انتخاب کرده و سپس روی Create and submit a request to this CA کلیک می کنیم.
- حال باید فرم ظاهر شده را پر و submit کرد.

- برای نصب کردن دستی **Certificate** صادر شده برای یک کامپیوتر، روی آن کامپیوتر:

- **Cmd** را با دسترسی مدیر، باز می کنیم و وارد می کنیم: **mmc**
- **Add or Remove Snap-ins** را باز کرده و از سمت چپ، گزینه ی **Certificates** را به شکل **Computer account** اضافه و باز
- می کنیم. در کادر سمت چپ، وارد شده و پوشه ی **Personal** را نیز باز کرده و کلیک راست کرده و **All Task** و سپس **Import** را
- می زنیم و **Certificate** موردنظر را وارد می کنیم.

- برای نصب کردن دستی **Public Certificate** بر روی یک کامپیوتر:

- همانطور که می دانیم، برای اینکه –معمولاً در شبکه های **Work group**–، **Client** ها به **CA Server** اعتماد داشته باشند، نیاز به
- **Public Certificate** آن **CA Server** خواهد بود.
- پس می توان در همان صفحه ی اول، گزینه ی **Download a CA certificate chain, or CRL** را انتخاب کرد.
- گزینه ی **Download CA certificate** را انتخاب می کنیم.
- برای **Import** کردن این **public certificate**، به **MMC** رفته و کنسول **Certificate** را فراخوانی می کنیم.
- به **Trusted Root Certifications Authorities** و روی **Certificates** کلیک راست کرده و **All tasks** و **Import** را می زنیم.
- توسط **Browse** گواهی **public** را وارد می کنیم و ویزارد را به پایان می رسانیم.

3. Group Policy:

- وارد **DC** شبکه شده و به کنسول **Group Policy Management** می رویم.
- وارد تنظیمات **Default Domain Policy** شده و به مسیر زیر می رویم:

Computer Configuration > Policies > Windows Settings > Security Settings > Punlic Key Policies > Trusted Publichers

- روی همین پوشه ی آخر کلیک راست کرده و **Import** را می زنیم.
- فایل **public Certificate** مربوط به **CA Server** را در اینجا وارد کرده و تمام.
- حال کافی ست همه ی **Client** ها یکبار تنظیمات **Group policy** را از نو دریافت کنند، (مثلاً پس از یکبار **restart**) همگی نسبت به **CA**، اعتماد پیدا خواهند کرد.

Certificate Templates :

در حقیقت یکی از تفاوت های نسخه ی **Enterprise** با **Stand alone** سرویس **CA** این است که نسخه ی **Enterprise** دارای پوشه ای به نام **Template Certificates** می باشد که شامل **Certificate** هایی از پیش تعریف شده است که می توان آنها را به دلخواه **modify** کرده و **Issue** و استفاده کرد.
پس کافی ست که روی آن کلیک راست کرده و **manage** را بزنیم.
نکته ی مشترکی که همه ی **Template Certificate** ها دارند این است که وقتی وارد **Properties** و تب **Security** آنها می شویم، می بینیم که برای **Authenticated User** ها، قابلیت **Read** فعال است که باید اینگونه باشد.

- برای استفاده از **Template** ها، باید از آنها یک **Duplicate** ایجاد کرد که با کلیک راست و **Duplicate** امکانپذیر است.
- پس از **Duplicate** باید وارد تب **General** شده و یک نام مناسب تعریف کرد.
- برای **issue** یا انتشار یک **Certificate** که از یک **Template** کپی شده است، باید روی پوشه ی **Certificate Templates** کلیک راست کرده و **new Certificate Template to issue** را بزنیم تا به لیست این کنسول اضافه شود.

- **Certificate Template** ها فقط در همان **Forest** معتبر هستند.
- **Certificate Template** ها غیر قابل حذف هستند.
- بطور پیش فرض فقط گروه **Enterprise Admins** و **Domain Admins** می توانند **Certificate Template** ها را مدیریت کنند.
- اگر چندین **Enterprise CA** داشته باشیم، هر تغییری در **Certificate Template** ها ایجاد کنیم، بر روی **Enterprise CA** های دیگر نیز ا اعمال می شود.
- **Certificate Template** ها در کل ساختار دومین **Publish** می شوند و هر **Subject** ای می تواند **Certificate Template** ها را طبق مجوزی که بر روی **Certificate** تنظیم شده است، **Enroll** کند.

ترفند :
برای مدیریت **Certificate Template** ها در ساختارهای چند دومینی می توان یک گروه برای این منظور ایجاد کنید و مجوز مدیریتی را به این گروه واگذار کرد.

Subordinate CA:

برای اینکه حجم و فشار کاری **Root CA** را کاهش دهیم، نیاز به **Subordinate Certification Authority** ها داریم.
پس برای هر بخش مشخص از وظایف، یک **Subordinate** ایجاد می کنیم، و کاربران برای درخواست هایشان بطور مستقیم با این **Subordinate** ها در ارتباط خواهند بود.

- از طرف دیگر، **Root CA** به سادگی می تواند برای امنیت بیشتر **offline** باشد، اما **SubCA** ها بدون هیچ خللی، به کار خود ادامه می دهند.
- پس به این دلیل که **Sub CA** ها با حجم زیادی عملیات و درخواست ها مواجه هستند، نیاز به راه اندازی یک وبسایت بروی آنها داریم.
- برای راه اندازی این وبسایت، اگر بخواهیم بصورت دستی عمل کنیم، **Implementation** یک سری پیشنیازها ضروری می باشد.
- باید دو افزونه (**Extension**) را روی **Root CA** ثبت کنیم و اعلام کنیم که انجام این دو، بر عهده ی کدام **SubCA** می باشد:

❖ Certificate Revocation List (CRL):

- در این لیست، **Certificate** هایی که قبل از تاریخ انقضایشان، لغو شده اند، لیست می شوند.
- وقتی یک کاربر، یک **Certificate** را از **SubCA** درخواست می کند، **SubCA** آن درخواست را در لیست **CRL** جستجو می کند.
- اگر در **CRL** وجود داشته باشد، یک **Error** مبنی بر رد درخواست، برای کاربر پس می فرستد.
- اگر در **CRL** وجود نداشته باشد، یک پیغام به نام **200OK** مبنی بر پذیرش درخواست، پس می فرستد.

✓ برای اینکه یک **SubCA** بتواند **Certificate** های تخصیصی به کاربران را، خودش ثبت یا **enroll** کند، باید تبدیل به یک **Web Server** شود که **CRL** آن کاملاً **update** باشد.

✓ پس **RootCA** باید لیست **CRL** را ایجاد کرده و در اختیار **SubCA** قرار دهد، و آدرس این **SubCA** را درون خودش ذخیره کند.

❖ Authority Information Access (AiA) :

این سرویس، شامل یک سری اطلاعات در مورد دریافت و ارائه ی هریک از **Certificate** ها می باشد.
به نوعی یک **Method** برای دریافت **Certificate** است.

Subordinate CA Implementation :

1. ابتدا باید سرویس AD CS را به عنوان Root CA نصب کرده باشیم.

باید دو Extension مربوط به CRL و AiA را درون Root CA تعریف کنیم.

برای اضافه کردن Extension ها در Root CA :

وارد کنسول Certification Authority می شویم.

در کادر سمت چپ، وارد Properties گزینه ی Root CA می شویم.

در تب Extensions، و در Select Extensions، گزینه ی .. CRL Distr.را انتخاب کرده و روی Add می زنیم.

در نوار Location، یک آدرس دلخواه در شبکه ی Domain خودمان، که با //:http شروع شود، و به یک پوشه به نام cdp برسد، درج می کنیم.

http://نام دلخواه.payamavar.local/cdp/

بطور معمول این نام دلخواه را pki قرار می دهند:

http://pki.payamavar.local/cdp/

حال در قسمت Variable گزینه ی <CaName> و سپس گزینه ی <CRLNameSuffix> را Insert می کنیم.

حال در پایانِ نوار Location به عنوان پسوند، درج می کنیم: .crl و OK را می زنیم.

حال گزینه ی .. Include in the CDP Extension of را فعال می کنیم.

یکبار Apply می کنیم، اما اجازه ی restart نمی دهیم.

در نوار Select Extensions، گزینه ی AIA را انتخاب کرده و روی Add می زنیم.

در نوار Location، یک آدرس دلخواه در شبکه ی Domain خودمان، که با //:http شروع شود، و به یک پوشه به نام aia برسد، درج می کنیم.که این آدرس دلخواه نیز معمولاً pki درج می شود.

http://pki.payamavar.local/aia/

حال در قسمت Variable گزینه ی <CaName> و سپس گزینه ی <CertificateName> را Insert می کنیم.

حال در پایانِ نوار Location به عنوان پسوند، درج می کنیم: .crt و OK را می زنیم.

حال گزینه ی .. Include in the AIA Extension of را فعال می کنیم.

باید Revokation List را برای Root CA ایجاد یا publish کنیم.

پس در در کنسول Certification Authority، از زیرگزینه های نام CA ایجاد شده، روی پوشه ی Revoked Certificates کلیک راست کرده و All Tasks و publish را می زنیم و new CRL را انتخاب کرده و OK.

حال باید CRL و البته CA Root را در اختیار Subordinate قرار دهیم.

هم می توان آنها را برای امنیت بیشتر، توسط یک رسانه ی ذخیره سازی مثل USB جابجا کرد، و هم می توان آنها را درون یک پوشه ی Share قرار داد؛ با دسترسیِ کاربر مجاز موردنظر بصورت Read and Write.

برای دسترسی به این دو فایل، باید به مسیر زیر رفت:

C:\Windows\System32\CertSrv\CertEnroll

2. باید Server ای که قرار است Subordinate شود را تنظیم کنیم.

- ابتدا نقش AD CS را نصب کنیم.

نکته: برای ایجاد یک Subordinate، ابتدا باید سیستم، عضوی از Domain شده باشد، چون پس از نصب AD CS، دیگر قادر به join شدن به Domain نخواهد بود.

3. بجز AD CS گزینه ی نقش IIS را نیز فعال می کنیم که نصب شود.

نکته: چون این Sub CA، قرار است که Certificate ها را تحت وب به Client ها ارائه دهد، در هنگام نصب AD CS، در قسمت Role Services، علاوه بر گزینه ی Certification Authority، گزینه ی Certification Authority Web Enrollment را نیز فعال می کنیم، که گزینه های سرویس IIS را نیز نصب خواهد کرد.

- پس از اتمام نصب، وارد بخش Configuration شده و تیک هر دو Service را فعال می کنیم.
- ترجیحاً آن را روی Enterprise قرار می دهیم. (به دلیل امکاناتی که ارائه می دهد.)
- Subordinate CA را انتخاب می کنیم.
- Create a new Private Key را می زنیم.
- تنظیمات Cryptography را تغییر نمی دهیم.
- و به تب Request a Certificate from Parent CA می رسیم:

4. در حقیقت ما باید به این Subordinate یک اعتبار بدهیم؛ به یکی از دو روش زیر:

- اگر Root CA هم Online باشد، می توان نام آن را در Parent CA درج کرد تا بطور خودکار این درخواست اعتبار را صادر کند.
- اما بطور offline گزینه یSave a Certificate Req.را می زنیم.
- بهرحال مراحل این نصب را تا پایان می رویم.
- حال یک فایل با پسوند req در دایرکتوری که تعیین شده بود، ایجاد می کند.
- این فایل، یک درخواست اعتبار از Root CA است؛ که باید آن را به Root CA برده و در آنجا ثبت کنیم؛ تا بتوانیم یک Certificate برای این Sub CA ایجاد کنیم و آنرا معتبر کنیم.
- فایل .req ایجاد شده را می توان به یکی از دو طریقی که در بالا گفته شد، به Root CA رساند.
- در Root CA، در کنسول Certification Authority، بر روی نام CA کلیک راست و All Tasks را زده و سپس گزینه ی Submit a new Request را زده و فایل .req را انتخاب می کنیم.
- حال این فایل در پوشه ی Pending Requests ایجاد می شود.
- پس روی آن کلیک راست کرده و All Tasks و issue را می زنیم که به پوشه ی Issued Certificates می رود.

5. حال باید این Certificate را به Sub CA برده و نصب کرد.

- پس در پوشه ی issued Cert.روی آن دابل کلیک کرده و در تب Details گزینه ی Copy to File را می زنیم، Next.
- گزینه ی ..Cryptographic Message Sy را و همچنین .. Include all Certificates in را فعال می کنیم.
- یک آدرس را انتخاب و یک نام برای آن تعیین می کنیم تا ذخیره شود، و سه فایل ایجاد شده را به Sub CA می بریم.

6. حال در SubCA ابتدا باید Root CA را نصب کنیم.

- پس روی فایلی که با نام و آدرس کامل Root CA است، کلیک راست کرده و Install Certificate را می زنیم.
- قاعدتاً Local Machine را می زنیم.
- باید تعیین کنیم که این Certificate مربوط است به همه ی CA هایی که قابل اعتماد هستند، پس Browse را زده و پوشه ی Trusted Root Certification A.را انتخاب می کنیم؛ و Next و Finish .
- برای نصب فایل Certificate دیگر که نام آن را خودمان تعیین کردیم، در همان سیستم Sub CA به کنسول Certification A می رویم.
- روی نام سیستم Sub CA کلیک راست کرده و All Tasks و Install CA Certificate را می زنیم؛ و فایل Certificate دوم را Open می کنیم.

7. حال باید تنظیمات IIS را انجام دهیم، پس ابتدا پوشه هایی مشابه با پوشه های یک وبسایت را ایجاد می کنیم.

- پس به درایو C و پوشه ی inetpub و سپس wwwroot می رویم.
- پوشه ای به نامی که برای extension ها ایجاد کرده بودیم، ایجاد می کنیم: pki
- درون این پوشه، دو پوشه به نام های aia و cdp ایجاد می کنیم.
- حال باید اجازه ی دسترسی برای پوشه ی pki را به گروه کاربران Cert Publichers بدهیم.
- پس وارد properties و تب Security و سپس Edit شده و با گزینه ی Add این گروه را اضافه کرده و دسترسیِ آن را Full control می کنیم.
- حال فایل Root CA (که با نام و آدرس کامل Root CA است) را به درون پوشه ی aia انتقال می دهیم.
- فایل Revokation List را که نام آن، آدرس Distinguished سیستم RootDC است را به پوشه ی cdp انتقال می دهیم.
- حال در همین Sub CA، به سرور IIS می رویم.(Tools > Internet Information Services Manager)
- در کادر سمت چپ، بر روی نام DC کلیک راست کرده و Add Website را می زنیم.
- Site Name را برابر با pki قرار می دهیم.
- برای Physical Path، به مسیر wwwroot رفته و پوشه ی pki را انتخاب می کنیم.
- برای Host Name، نامی که درج کردیم را همراه با نام کامل Root DC درج می کنیم:

pki.payamavar.local

- Type باید روی http و Port باید روی 80 قرار داشته باشد.
- گزینه ی Start Website immediately را فعال کرده و OK و تمام.

8. حال باید نامی که برای Host Name تنظیم کردیم را در DNS تنظیم کنیم.

- پس به main DC برگشته و وارد کنسول DNS می شویم.
- در پوشه ی Forward Lookup Zones، بر روی پوشه ی Root Domain کلیک راست کرده و New Host.
- برای Name درج می کنیم : pki و برای IP Address هم IP مربوط به سیستم Sub CA را وارد می کنیم.
- گزینه ی .. Create associated pointer را فعال می کنیم و Add Host را می زنیم.

9. به سیستم Sub CA برگشته و وارد کنسول Certification Authority می شویم.

- روی نام Sub CA ایجاد شده کلیک راست کرده و All Tast و Start Service را می زنیم تا این سرویس بکار بیفتد.

Root CA Publishment توسط Group Policy :

در حقیقت ما می توانیم پس از ایجاد Root CA، آن را از طریق GPO ها، در محیط شبکه و بین DC های دیگر share کنیم.
در GP Management وارد Default Domain Policy می شویم.
به مسیر زیر می رویم:

Computer Configuration > Policies > Windows Setting > Security Setting > Public Key Policies > Trusted Root CAs

درون آن، راست کلیک کرده و Import را زده و فایل Root CA که در کنسول Certification A.و پوشه ی Issued Certificates با نام و آدرس کامل Certificate ایجاد شده بود را انتخاب می کنیم و تا پایان پیش می رویم.

: Automatic Enrollment the Certificates

به مسیر زیر می رویم:
Computer Configuration > Policies > Windows Setting > Security Setting > Public Key Policies >
وارد properties گزینه ی Certificate Services Client – Auto Enrollment شده و آنرا Enable کرده و تیک گزینه های آنرا فعال می کنیم.

: Online Responder

- به عنوان جایگزین CRL نیز از Online Responder می توان استفاده کرد.
- Online Responder می تواند اطلاعات مربوط به وضعیت یک Certificate را که لغو اعتبار شده است، برای مدیر شبکه فراهم کند، در حالیکه CRL فقط لیست Certificate های لغو اعتبار شده را فراهم می کند.

  - Online Responder نباید روی کامپیوتری نصب شود که Certification Authority روی آن نصب می باشد!
  - یعنی این دو Role Service نباید روی یک کامپیوتر واحد نصب شوند، و یا حداقل نباید روی Root DC این سرویس را نصب کرد.
  - چون بهتر است که کامپیوتر DC را درگیر این کارها نکنیم.

برای نصب Online Responder در کنسول Server Manager روی Add roles and features کلیک کرده و در صفحه Role Server از زیرگزینه های Active Directory Certificate Services، گزینه ی Online Responder را فعال می کنیم.
تعدادی کامپوننت Web نیز نصب می شوند.
برای پیکربندیِ آن، در کنسول server manager در قسمت notification روی Configure Active Directory Certificate Services کلیک می کنیم و ویزارد را تا پایان می رویم.

حال در سیستم Sub CA ، وارد کنسول Certfcn Authrty شده و با کلیک راست بر روی Certificate Templates گزینه ی new و سپس Certificate Template to issue را می زنیم و سپس از لیست موجود، گزینه ی OCSP Response Signing را انتخاب کرده و OK!

Task distribution برای Certificate ها:

در حقیقت بطورپیشفرض هیچ گروه کاربری ای برای اینکه تعیین کنیم چه افرادی مجاز به ایجاد Certificate ها هستند یا خیر، وجود ندارد.
پس می توانیم خودمان یک گروه Global به نام مثلاً Cert-issuer ایجاد کنیم و در کنسول Certification A. روی نام DC کلیک راست کرده و وارد Properties و تب Security شده و گروه مورد نظر را Add کرده و سطح دسترسی را بر روی Issue and manage Certificates قرار می دهیم.

:Certification Authority Backup

- روی نام **DC** در کنسول **Certification Authority** کلیک راست کرده و **All Tasks** و **Back up CA** را می زنیم.
- تیک گزینه های **Private Key** ها و **Certificate database** ها را فعال می کنیم.
- یک آدرس برای ذخیره ی این **Backup** تعیین کرده و یک **Password** برای زمان **Restore** آن تعیین کرده و تمام!
- نکته: عملیات **Back up** بدون اینکه باعث خللی در کار کنسول **CA** ایجاد کند، آغاز می شود.
- اما برای عملیات **Restore**، کنسول **CA** باید **Stop** شود.

Routing :

مسیریابی در شبکه، زمانی تبدیل به یک چالش می شود که بیش از یک **Subnet** در شبکه داشته باشیم.
در حقیقت هر **Subnet** را می توان یک شبکه ی مجزا در نظر گرفت.
به ازای هر **Subnet** یک **Default Gateway** وجود خواهد داشت.

در حالت استاندارد، به این شکل عمل می کنیم که **Client** ها را در یک **Subnet** و **Server** ها را در یک **Subnet** مخصوص به خود قرار دهیم.
و در ادامه اگر **Client** های **wireless** هم داشته باشیم، می توانیم آنها را نیز در یک **Subnet** اختصاصی خود قرار دهیم.

ارتباطات درون یک **Subnet** ، به سادگی و با قرار دادن یک **Switch** لایه دو برقرار می شوند که فقط کافیست **Client** ها به آن متصل شوند.
اما اگر دو کامپیوتر در **Subnet** های مختلفی قرار داشته باشند، حتی اگر به یک سوئیچ مشترک متصل باشند، قادر به ارتباط با یکدیگر نخواهند بود.
می توان برای شبکه های کوچک، به صورت نرم افزاری و از طریق ابزارهای **Microsoft** اقدام به پیاده سازی یک **Router** نرم افزاری کرد.**RRAS** یک ابزار برای پیاده سازی یک **Router** نرم افزاری با استفاده از امکانات **Windows Server** است.

Router چه سخت افزاری باشد و چه بوسیله ی ویندوز شبیه سازی شده باشد، نیازمند یک یا تعدادی درگاه (Interface) فیزیکی شبکه خواهد داشت.
هر کابلی که توسط یک درگاه، به **Router** وصل می شود، می تواند نماینده ی یک شبکه ی متفاوت از شبکه ی پشت درگاه های دیگر موجود درشبکه باشد.

❖ برای دریافت لیست **NIC** ها یا پورت های شبکه ی موجود روی دستگاه، همراه با خلاصه ای از مشخصات مهم آنها:

cmd	ipconfig
PowerShell	`Get-NetAdapter | select status,ifIndex, Name,InterfaceDescription, LinkSpeed, MacAddress, PhysicalMediaType ,DriverName | Format-Table -AutoSize`

❖ برای دریافت لیست **NIC** های موجود روی دستگاه، همراه با آدرس **IP** آنها و نحوه ی دریافت **IP** که دارند:

cmd	Ipconfig /all
PowerShell	`Get-NetIPAddress -AddressFamily IPv4 | select InterfaceIndex, InterfaceAlias, AddressFamily, IPAddress, PrefixLength,PrefixOrigin,SuffixOrigin`

❖ برای دریافت مشخصات مهم **NIC های روشن و فعال روی سیستم**، تنها کافی ست **Script** زیر را اجرا کنیم:

```
#Displays IP and DNS address configs on any UP-NIC:
$UpNICs=Get-NetAdapter | % { Process { If (( $_.Status -eq "up" )){ $_.InterfaceAlias}}}
foreach($NIC in $UpNICs){
Get-NetIPConfiguration -InterfaceAlias $NIC
}
```

نکته: درحقیقت Interface Index یا همان **ifIndex** ، یک شماره ی شناسایی منحصربفرد برای هر NIC فیزیکی یا مجازی روی سیستم است، که برخی دستورها یا نرم افزارها، تنها توسط این شماره، ارتباط با NIC ها را کنترل می کنند.

همه ی **Router** ها یک جدول مسیریابی (Routing Table) دارند، که نوعی **Router** نرم افزاری می باشد.

❖ برای مشاهده ی جدول مسیریابی Router نرم افزاری موجود در Windows از دستور زیر استفاده می کنیم:

cmd	Route print
PowerShell	`Get-NetRoute`

:Route print

❖ Interface List :

❖ لیست آداپتورهای موجود روی سیستم را می بینیم. (NIC) که قبل از نام، شماره ی IfIndex و mac address آنها قرار دارند.

❖ در دو قسمت زیر، لیست مسیرهای ثبت شده ی روی این سیستم را برای آدرس های v4 و v6 می بینیم:

IPv4 Route Table و IPv6 Route Table

نکات:

❖ برای مشاهده ی فقط تنظیمات IPv4 و یا فقط IPv6 در جدول مسیریابی:

Route Print -4
Route Print -6

❖ برای مشاهده ی تنظیمات فقط آدرس هایی که با 192.168 شروع می شوند:

Route Print 192.168.*

❖ آدرس 0.0.0.0 به معنی «**همه ی آدرس ها**» می باشد.

❖ آدرس 255.255.255.255 اگر برای **مقصد** باشد، به معنی «**Broadcast address**» می باشد.

❖ آدرس 255.255.255.255 اگر برای **Netmask address** باشد، به معنی «**تنها همان یک آدرس**» می باشد.

❖ Active Routes :

✓ ستون **Network Destination**، آدرس هایی که نرم افزارها و یا خود کاربر، جهت دسترسی، درخواست می کنند را مشخص می کند.

✓ ستون **Net mask**، آدرس Subnet mask مربوط به مقصد درخواست شده را مشخص می کند.

✓ ستون **Interface**، آدرس NIC ای که درخواست را به سمت آن هدایت می کند، مشخص می کند.

✓ ستون **Gateway**، آدرس Router ای که درخواست، به سمت آن هدایت خواهد شد را مشخص می کند.

در اینجا، وقتی عبارت On-link درج شده باشد، یعنی هدایت بسته ی درخواست، برعهده ی خود NIC، خواهد بود.

✓ ستون **Metric**، هزینه یا Cost مربوط به Route را مشخص می کند.

✓ میزان Cost هر Route با مشخصه های خاصی مثل سرعت و تعداد node های بین راه تعیین می شود.

هرقدر که میزان metric یک مسیر کمتر باشد، در اولویت تر خواهد بود.

برای اطلاع دقیق تر از مفهوم ارقام metric ها، می توان در Google، عبارت زیر را بر اساس نسخه ی ویندوز، جستجو کرد:

the link speeds and assigned metrics for computers that run Windows X

✓ **به ازای هریک NIC فعال روی سیستم، یک مسیر برای هدایت همه ی درخواست ها، به شکل زیر ایجاد می شود:**

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.X.1	192.168.X.X	X

✓ **:Loopback Routes**

با توجه به سه Route زیر، که همیشه بطورخودکار روی سیستم ایجاد می شوند، تمام IP های موجود در بازه ی 127.0.0.0 **تا** 127.255.255.255 **، برای Loopback رزرو شده اند، و بطورمستقیم به** 127.0.0.1 **ارجاع داده می شوند.**

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	On-link	127.0.0.1	X
127.0.0.1	255.255.255.255	On-link	127.0.0.1	X
127.255.255.255	255.255.255.255	On-link	127.0.0.1	X

مثال: در **Routing table** زیر، می بینیم که دو **NIC** روی سیستم فعال هستند:

```
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.139.2  192.168.139.144    281
          0.0.0.0          0.0.0.0    192.168.178.1   192.168.178.55     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.139.0    255.255.255.0         On-link   192.168.139.144    281
  192.168.139.144  255.255.255.255         On-link   192.168.139.144    281
  192.168.139.255  255.255.255.255         On-link   192.168.139.144    281
    192.168.178.0    255.255.255.0         On-link    192.168.178.55    281
   192.168.178.55  255.255.255.255         On-link    192.168.178.55    281
  192.168.178.255  255.255.255.255         On-link    192.168.178.55    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.139.144    281
        224.0.0.0        240.0.0.0         On-link    192.168.178.55    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.139.144    281
  255.255.255.255  255.255.255.255         On-link    192.168.178.55    281
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0    192.168.139.2  Default
          0.0.0.0          0.0.0.0    192.168.139.2     256
===========================================================================
```

✓ می بینیم که مسیر زیر، نشان می دهد، هر بسته ای که مقصدش، در شبکه ی خود **NIC** باشد، به سمت خود **NIC** ارسال می شود. یعنی خود **NIC**، هدایت بسته هایی که در شبکه ی خودش هستند را برعهده می گیرد.

Network Destination	Netmask	Gateway	Interface	Metric
192.168.139.0	255.255.255.0	On-link	192.168.139.144	X
192.168.178.0	255.255.255.0	On-link	192.168.178.55	X

در اینجا، آدرس IP خود NIC برابر است با: 192.168.139.144

✓ در صورتی که مقصد یک بسته، برابر با آدرس خود **NIC** و یا آدرس **broadcast** آن باشد نیز، به سمت خود **NIC** هدایت می شود:

Network Destination	Netmask	Gateway	Interface	Metric
192.168.139.144	255.255.255.255	On-link	192.168.139.144	X
192.168.139.255	255.255.255.255	On-link	192.168.139.144	X
192.168.178.55	255.255.255.0	On-link	192.168.178.55	X
192.168.178.255	255.255.255.0	On-link	192.168.178.55	X

✓ Multicast Routes:

درحقیقت گاهی ممکن است نرم افزار یا سرویسی، نیاز داشته باشد که بسته ای را به شکل **multicast** در شبکه ارسال کند؛ به همین جهت از آدرس 224.0.0.0 که یک آدرس **multicast** است، استفاده شده و به شکل خودکار به ازای هریک از **Interface ها به** اضافه ی **loopback Interface**، یک **Multicast route** ایجاد می شود.

✓ Broadcast Routes:

درحقیقت گاهی ممکن است نرم افزار یا سرویسی، نیاز داشته باشد که بسته ای را به شکل broadcast در شبکه ارسال کند؛ به همین جهت آدرس مقصد آن بسته را 255.255.255.255 تعیین می کند. به همین دلیل، همیشه بر روی Windows، به شکل خودکار به ازای هریک از Interface ها به اضافه ی loopback Interface، یک Broadcast route ایجاد می شود.

- **Persistent Routes :**

در هر سیستم، یک سری Route مشخص و پایدار، تعریف شده است، که آنها را در این کادر مشاهده می کنیم.

- **وقتی به شکل دستی، یک static Route ایجاد می کنیم، و قصد داریم این مسیر در Routing Table سیستم ثبت شده و با Restart یا قطع و وصل شدن ارتباط شبکه، از بین نرود، آن را به این قسمت منتقل می کنیم.**
- **و یا وقتی metric یک مسیر را عدد یک تعریف کنیم، تبدیل به یک مسیر دایمی شده و به این قسمت منتقل می شود.**
- **پس مسیری که در این قسمت قرار دارد در اولویت ترین مسیر نیست** (حتی با داشتن metric برابر با یک).

بطور ترجیحی بهتر است که هر persistent Route، بازه ی آدرس IP (Subnet mask)**محدودی را شامل شود ، نه یک بازه ی بلند مثل** 0.0.0.0 **و یا حتی نه مثل** 255.255.255.0 **را.**

همیشه اولویت بندی انتخاب یک Route برای رسیدن به یک مقصد، بر اساس مسیرهای قسمت Route Table است.

Work on Routes :

مشاهده ی مسیرها:

- دستور زیر، معادل دستور Route print اما برای PowerShell است، که قابلیت های بهتری خواهد داشت:

```
Get-NetRoute
```

در نتیجه ی این دستور، ستون های ظاهر شده، معادل ستون های دستور route print هستند:

DestinationPrefix	ifMetric	NextHop	
Network Destination	Metric	Gateway	

نکته: دستور **Get-NetRoute**، مسیرهای مربوط به همه ی NIC های موجود را لیست می کند، حتی آنها که خاموش یا حتی بی کاربرد هستند.
پس می توان از اسکریپت زیر هم استفاده کرد تا تنها، Route های مرتبط به NIC های روشن را دریافت کنیم:

```
$UpNICs=Get-NetAdapter | % { Process { If (( $_.Status -eq "up" )){ $_.InterfaceAlias}}}
foreach($NIC in $UpNICs){
Get-NetRoute -AddressFamily IPv4 -InterfaceAlias $NIC }
```

نکته: جهت بررسی اینکه آیا یک Route درست کار می کند یا خیر، بهترین دستور، tracert می باشد، که پیشروی به سمت مقصد را گام به گام (Gateway به Gateway) نشان می دهد.
مثلن جهت بررسی اینکه آیا سیستم جاری، جهت رسیدن به آدرس 10.10.3.2 از مسیر موردنظرمان عبور می کند یا خیر، دستور زیر را وارد می کنیم.
همان اولین گام ظاهر شده، مشخص می کند که عبور می کند یا خیر:

```
tracert 10.10.3.2
```

ایجاد یک Route :

مثلاً می خواهیم همه ی بسته هایی که به مقصد 192.168.178.0/24 **می روند، به NIC به آدرس** 192.168.178.90، که Interface Index **آن، عدد 5 است، هدایت شوند:**

```
route add 192.168.178.0 mask 255.255.255.0 192.168.178.90 IF 5
```

البته این Route یک مسیر موقتی محسوب می شود، و با قطع و وصل شدن اتصال network و یا حتی با یکبار restart کردن سیستم، از بین می رود. پس می توانیم در انتهای این دستور، از سوییچ p- استفاده کنیم:

```
route add 192.168.178.0 mask 255.255.255.0 192.168.178.90 IF 5 -p
```

می بینیم که این Route هم به کادر Persistent Routes اضافه شده است.

ایجاد همین Route در PowerShell:

```
New-NetRoute -DestinationPrefix 192.168.178.0/24 -InterfaceIndex 5 -NextHop 192.168.178.1
```

تغییر یک Route :

یک مثال برای cmd:

```
route change 192.168.9.0 mask 255.255.255.0 192.168.5.215 IF 11 -p
```

یک مثال برای PowerShell:

```
Set-NetRoute -DestinationPrefix 0.0.0.0/0 -InterfaceIndex 20 -NextHop 192.168.5.215 -RouteMetric 25 -Publish Yes
```

نکات:

- اگر مسیری موجود نباشد، نمی توان آن را تغییر داد.
- بطورپیشفرض، گاهی metric مربوط به NIC ها، از یک عدد خاص شروع می شود، و هرقدر که ما توسط دستور بالا، metric آن را تغییر دهیم، عددی که وارد می کنیم، تنها به مقدار پیشفرض اولیه ی آن افزوده می شود.
- مسیرهای مرتبط با wireless NIC ها، همیشه مقداری کمتر از metric مربوط به NIC های کابلی است.
- پس برای در اولویت قرار دادن یک Route که از یک wireless NIC گذر می کند، لازم است که metric مربوط به wired NIC را از آن بیشتر تنظیم کنیم.

حذف یک Route :

یک مثال برای cmd:

حذف مسیری که «همه ی درخواست های به شبکه ی 192.168.9.0 را روی NIC به شماره ی 5 و به Gateway به آدرس 192.168.5.215» ارسال می کند:

route delete 192.168.9.0 mask 255.255.255.0 192.168.5.215 IF 5 -p

یک مثال برای PowerShell:

حذف مسیری که «همه ی درخواست ها را روی NIC به شماره ی 24 و به Gateway به آدرس 192.168.178.1» ارسال می کند:

```
Remove-NetRoute -DestinationPrefix 0.0.0.0/0 -InterfaceIndex 24 -NextHop 192.168.178.1
```

برای ایجاد دوباره ی همین مسیر:

```
New-NetRoute -DestinationPrefix 0.0.0.0/0 -InterfaceIndex 24 -NextHop 192.168.178.1
-RouteMetric 5 -Publish Yes
```

: Windows Routing issues

:Reset the TCP/IP

می دانیم که پروتکل TCP/IP مسیول مدیریت DNS address ، IP address، Subnet mask ، Default Gateway و Route های موجود روی سیستم ها می باشد، که از گزینه های اصلی ارتباط شبکه ای هستند.

:گاهی ممکن است

- **به دلیل قطع و وصلی ها و یا ارتباط با Gateway های متفاوت، جدول Routing Table سیستم بهم ریخته و یا شلوغ شده باشد.**
- **سیستم یک آدرس IP تکراری در شبکه را دریافت کرده باشد.**

درنتیجه دسترسی به برخی از سرویس ها یا نقاط در شبکه، دچار اختلال شده باشد و یا حتی کاملن قطع شود.

:در این زمان، می توان سرویس TCP/IP را توسط دستور زیر، یکبار راه اندازی مجدد کرد

درحقیقت این راه اندازی مجدد، به این معنا خواهد بود که پروتکل TCP/IP یکبار کاملن حذف شده و از نوع ایجاد و راه اندازی می شود.

netsh int ip reset reset.txt

پس از اعمال این دستور، همه ی آدرس های Static IP و اطلاعات مربوط به آنها بر روی NIC ها، حذف می شوند.

:Reset the Winsock

گاهی نرم افزارهای تحت شبکه مثل VPN ها ، Browser ها، Email client ها و غیره، تغییرات ناخواسته ای را در تنظیمات مسیریابی یک سیستم اعمال می کنند که ارتباط سیستم با اینترنت یا شبکه، مختل خواهد شد، بطورمثال برخی یا بیشتر Web page ها قابل دسترسی نخواهند بود، درحالی که ارتباط با شبکه، همچنان صحیح و پایدار است.

درحقیقت در این موارد، یکی از بزرگترین احتمال ها وجود اختلال در Winsock Catalog **سیستم می باشد.**

در حقیقت Winsock یک API (Application Programming Interface) است که در میان نرم افزارها مثل Browser ها و پروتکل های ارتباطی کار می کند.

بطورکلی، Winsock تنظیمات مهم مربوط به چگونگی برقراری ارتباط میان یانک های داده ی نرم افزارها را درون Catalog خود ذخیره می کند.

پس وقتی اخلال در Winsock باعث عدم دسترسی به وبسایت ها شود، می توان Catalog آن، که محل ذخیره ی تنظیمات آن است را یکبار بارگذاری دوباره کرد. پس در cmd دستور زیر را وارد می کنیم:

netsh winsock reset

: Relay Agent

فرض کنید یک کامپیوتر را که دارای یک آدرس کاملاً متفاوت با آدرس Domain شبکه است، به شبکه متصل کنیم.
در حقیقت پس از اتصال سخت افزاری، هیچ ارتباطی میان این کامپیوتر و اعضای Domain برقرار نخواهد شد.
پس یا باید از یک دستگاه Router استفاده کنیم و یا یک Member Server را تبدیل به RRAS کنیم که به آن Relay Agent گفته می شود.

می دانیم که وقتی سیستمی به شبکه متصل می‌شود، درخواست IP خود را به صورت broadcast در شبکه ارسال می‌کند تا به دست DHCP Server برسد.
DHCP relay agent پروتکلی در Switch ها یا Router ها و یا قابلیتی ست که بر روی یک سیستم Server فعال می شود، برای انتقال پیام ها، بین Client هایی که IP Address های متفاوت با سیستم های دیگر شبکه دارند.
در حقیقت ما می توانیم در DHCP Server چندین Scope ایجاد کنیم، که هر یک از این Scope ها، Address Pool ها یا رنج های کاملاً متفاوت با Scope های دیگر داشته باشند.
همه ی کامپیوترهای شبکه، با هر نوع IP Address ای، باید از یک DHCP Server، آدرس IP دریافت کنند!
پس راهکار این است که در بالای تمام سیستم هایی که دارای رنج IP مشابه هستند، یک Server قرار دهیم که قابلیت Relay Agent را برای آن محدوده از IP، پشتیبانی کند.و در پایان همه ی آن Relay Agent Server ها را به DHCP Server اصلی شبکه متصل کنیم.
هر Relay Agent Server باید دارای دو کارت شبکه یا دو درگاه NIC باشد.
سیستم Relay Agent، پس از دریافت درخواست IP ای که بصورت Broadcast از Client ارسال شده است، چون محل DHCP Server موردنظر آن را می داند، درخواست او را به صورت unicast برای Server موردنظرش ارسال می کند.
Router ها به پیام های Unicast اجازه ی عبور می دهند!

راه حل بهینه تر این است که Router را تبدیل به یک DHCP Relay Agent کنیم.
درنتیجه هر درخواستی که به صورت Broadcast به Router می رسد، Router متوجه می شود که این درخواست با اینکه از نوع Broadcast است، اما برای دریافت IP فرستاده شده است، پس درخواست را دریافت کرده و آن را به Unicast تبدیل کرده و به DHCP Server اصلی که برایش تعریف شده است، ارسال می کند.در این حالت، به Router، BOOTP Relay Agent گفته می شود.

برای بکارگیری قابلیت Relay Agent در Router ها یا Switch ها، باید دستگاه موردنظر، قابلیت کار در لایه ی 3 شبکه را داشته باشد، چون دستگاه های لایه ی 2، قابلیت Relay Agent را پشتیبانی نمی کنند.
یعنی دستگاه مورد نظر باید قابلیت InterVLAN routing را پشتیبانی کند.
در واقع این نوع سوییچ ها، می توانند در نقش DHCP Server، DHCP Client و DHCP Relay Agent یا بصورت ترکیبی در شبکه حضور داشته باشد.

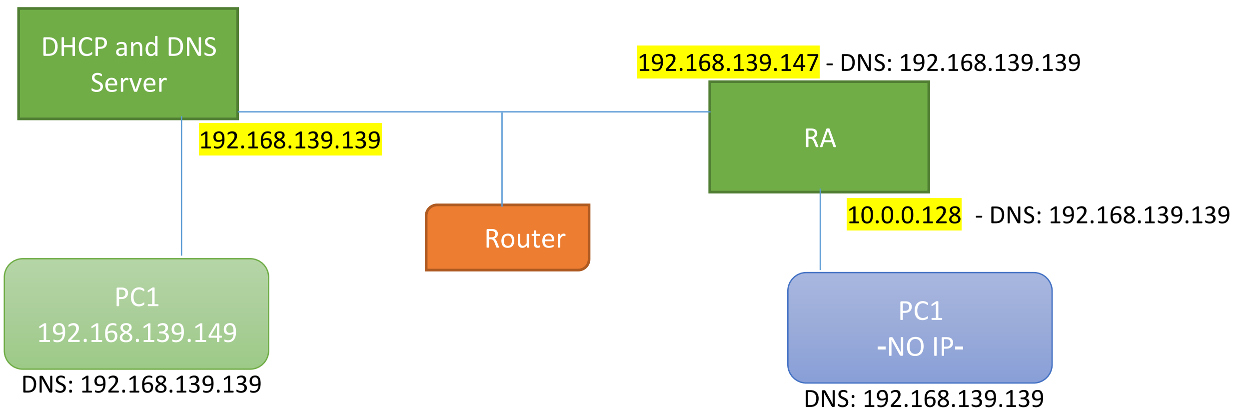
DHCP Relay Agent در سیسکو به عنوان IP Helper هم شناخته می شود.
اگر بخواهیم Relay Agent را کاملاً بصورت نرم افزاری در یک کامپیوتر انجام دهیم، نیاز به یک Router مجازی نیز خواهیم داشت که به آن RRAS یا Routing and Remote Access Service گفته می شود.
در حقیقت RRAS یک نرم افزار مسیریاب است که می تواند برای متصل کردن Network Segment ها به کار رود.
RRAS جهت دسترسی از راه دور کاربران به Server نیز امکاناتی را فراهم می آورد.
سرویس RRAS همراه با ویندوز Server نصب می شود، اما غیرفعال است، که تنها باید آن را توسط wizard مربوط به آن، فعال کرد.

پیشنیازهای کامپیوتر Relay Agent :

- باید دارای دو کارت شبکه باشد.
- دو سرویس ICF و ICS باید در آن غیرفعال باشند.چون RRAS با این دو سرویس نمی تواند کار کند.

: Deploy a Relay Agent

1. بر روی سیستم RA، که دارای دو NIC است، یک ویندوز Server نصب کرده و IP آن NIC ای که به سمت شبکه ی با رنج (مثلاً) 10.0.0.0 است، بر روی 10.0.0.128 قرار می دهیم.
2. در سیستم DHCP Server اصلی، یک Scope جدید برای شبکه ی با رنج 10.0.0.0 ایجاد می کنیم.
   - بر روی IPv4 کلیک راست کرده و new Scope را می زنیم.
   - یک نام و یک رنج IP متفاوت و دلخواه، برای آن تعیین می کنیم.مثلاً: 10.0.0.130 تا 10.0.0.150
   - می توانیم ترجیحاً Subnetting را براساس C Class تعیین کنیم، پس length را برابر با 24 قرار می دهیم.
   - آدرس Default Gateway آن را برابر با 10.0.0.128 قرار می دهیم.
   - چون می خواهیم همه ی این Client ها با هر دو نوع IP Address، از DHCP Server اصلی شبکه، IP دریافت کنند، پس DNS Address همه ی آنها را برابر با آدرس DHCP Server قرار می دهیم.



3. کنسول RRAS را بر روی سرور RA راه اندازی می کنیم.

نکته: باید این سرویس را در خود Server Manager سرور RA نصب و راه اندازی کرد که Error ندهد.

   - بر روی سیستم RA، از درون Server Manager وارد ویزارد Add Roles and Features می شویم.
   - در تب Server Roles گزینه ی Remote Access را انتخاب می کنیم.
   - در بخش Role Services، گزینه ی Routing را انتخاب می کنیم و تا پایان نصب پیش می رویم.
   - از منوی Tools، وارد گزینه ی Routing and Remote Access می شویم.

حال اگر در کادر سمت چپ این کنسول، آبجکت سرور RA موجود نبود، بر روی Routing and Remote Access کلیک راست و Add Server و سپس the Following Computer را زده و نام FQDN سرور RA را درج و OK می کنیم.
بر روی سرور اضافه شده، کلیک راست کرده و .Configure and enable Rout را می زنیم.
گزینه ی Custom Configuration را و سپس LAN Routing را انتخاب کرده و Finish و Start Service را می زنیم.

4. باید در RRAS تعریف کنیم که کدام Ethernet یا آداپتور NIC، متصل به DHCP Server شبکه و کدام متصل به Client های رنج 10.0.0.0 می باشد.
   - ابتدا باید قابلیت Relay Agent را فعال کنیم.
   - پس گزینه ی آبجکت RA را باز کرده و از زیرگزینه های IPv4، بر روی General کلیک راست کرده و New Routing Protocol را زده و گزینه ی DHCP Relay Agent را انتخاب و OK می کنیم.
   - باید DHCP Server شبکه را برای Relay Agent تعریف کنیم، پس وارد Properties آن شده و آدرس DHCP Server را وارد می کنیم. (که می شود همان 192.168.139.139)

- حال باید برای Relay Agent تعیین کنیم که به کدام شبکه گوش بدهد یا آنرا monitor کند.

پس روی آن کلیک راست کرده و New Interface را زده و Ethernet ای که مربوط به Client های رنج 10.0.0.0 است را انتخاب و OK می کنیم.

- گزینه ی Relay DHCP Packet را فعال نگه می داریم و OK می کنیم.

5. **حال Client های رنج 10.0.0.0 باید از Scope ای که برای این رنج در DHCP Server تعریف کردیم، IP دریافت کنند؛ اما نمی کنند!**

- **DHCP Server** درخواست های **Client** های **10.0.0.0** را مبنی بر اختصاص **IP Address** دریافت می کند.

(**DHCP Relay Agent** به خوبی کار می کند.) اما موقع پاسخگویی به آن **Client** ها:

- از یک طرف بسته های ارسالی **DHCP Server**، از طریق **Router** دور انداخته می شوند، چون ناشناس به نظر می رسند.
- از طرف دیگر پیام ها نمی دانند که راه رسیدن به **Client** های رنج **10.0.0.0** این است که از سرور **RA** عبور کنند.(که آدرسش 198.168.139.147 می باشد.)

6. **پس باید یک Static Route در DHCP Server برای درخواست های رنج 10.0.0.0 تعریف کنیم.**

- یعنی وقتی **DHCP Server** بخواهد پاسخی را به مقصد یکی از **Client** های **10.0.0.0** ارسال کند، از سیستم **192.168.139.147** عبور کند.
- این **Static Route** را باید بصورت **Persistent** (دائمی) تعریف کنیم.
- وارد **PowerShell** شده و دستور زیر را وارد می کنیم:

```
route add Scope ID mask SubnetMaskIP RelayAgentServerIP -p
```

- منظور از **Scope ID** : مربوط به **Scope** ای است که برای **Client** های با **IP** متفاوت ایجاد کرده بودیم: **10.0.0.0**
- منظور از **SubnetMaskIP** : آدرس **Subnet** آن **Scope** است.
- منظور از **RelayAgentIP** هم آدرس **IP** سرور **RA** است.
- منظور **-p** این است که این **Route** را بصورت **Persistent** ایجاد کن!

```
route add 10.0.0.0 mask 255.255.255.0 192.168.139.147 -p
```

- برای مشاهده ی این **Route** در لیست **Route** های دیگر **DHCP**، دستور زیر را وارد کرده و آنرا در بخش **Persistent Routes** مشاهده خواهیم کرد:

```
route Print
```

7. **حال کافی ست Ethernet سیستم PC1 را یکبار renew کنیم تا یک IP Address از Scope مربوط به خودش، دریافت کند.**

: Dynamic Update

وقتی که Relay Agent را برای یک سری Client با IP های متفاوت ایجاد کردیم، برای ثبت این IP های جدید در DNS Server باید بصورت دستی عمل کنیم!
برای اینکه بطور خودکار این آدرس های متفاوت در DNS Server شبکه هم ثبت و به روز شوند، باید در DHCP Server تعریف کنیم که هرگاه هریک از Object هایش در هرکدام از Scope هایش، عملیات renew انجام داد، آن را به DNS Server هم ارسال کرده و در آنجا هم ثبت شود.
فرض کنید در PowerShell، یک Reverse Lookup Zone برای Scope جدید ایجاد می کنیم:

```
Add-DnsServerPrimaryZone -ComputerName ifm -NetworkId '10.0.0.0/24' -ReplicationScope Domain
```

حال اگر به کنسول DNS برویم، می بینیم که Reverse Lookup Zone ایجاد شده است، اما Forward Lookup Zone ای برای آن ایجاد نشده است! پس به کنسول DHCP رفته و از درون Server اصلی، وارد Properties آبجکت IPv4 شده و در تب DNS، گزینه ی Always dynamically update DNS Records و گزینه ی ...Dynamically Update DNS را انتخاب و فعال می کنیم.

این تغییر در تب DNS را می توان از طریق PowerShell هم انجام داد.

```
Set-DhcpServerv4DnsSetting -ComputerName ifm -DynamicUpdates Always  -UpdateDnsRRForOlderClients $true
-DeleteDnsRROnLeaseExpiry $true
```

حال اگر یکبار در یکی از Client های رنج 10.0.0.0 (مثلاً سیستم PC1)دستور ipconfig /renew را وارد کنیم، و سپس هریک از دو دستور زیر را تست کنیم، پاسخ دریافت می کنیم:

Nslookup PC1

Nslookup 10.0.0.131

: Routing Protocols

روش هایی که شکل و حالت انتقال بسته های اطلاعاتی در شبکه را تعریف می کنند، «پروتکل های مسیریابی» نامیده می شوند.
دو روش مسیریابی کلی وجود دارد:

- مسیریابی ایستا یا Static Routing
- مسیریابی پویا یا Dynamic Routing

در مسیریابی static، بسته های اطلاعاتی فقط از همان مسیری که توسط مدیر شبکه تعریف شده اند، راهشان برای رسیدن به مقصد را پیدا می کنند و راه دیگری را نمی توانند پیدا کنند.
بطورمعمول Static Routing برای شبکه هایی با ابعاد کوچک استفاده می شود، اما مسیریابی پویا بیشتر در شبکه های بزرگ و به ویژه در اینترنت استفاده می شود.

در ساده ترین تعریف ، اگر Router های موجود در مسیر تشخیص دهند که مسیر بهتری برای رساندنِ بسته ی اطلاعاتی به مقصد وجود دارد، قطعا بسته را از آن مسیر عبور می دهند که معمولا با پیدا کردن کوتاه ترین مسیر بین مبدا و مقصد انجام می شود.

Dynamic Routing از Routing Protocol ها برای شناسایی شبکه ها و مقصدها و همچنین پیدا کردن بهترین مسیر برای رساندن بسته ها به مقصد استفاده می کنند.
Dynamic Routing این قابلیت را به Routing Table می دهد که بتواند زمانیکه یک Router خاموش است یا در دسترس نیست یا اینکه یک شبکه جدید به مجموعه اضافه می شود، این تغییرات را در Routing Table ها اضافه کند.

اگر شما در یک مسیریاب، یک Static Route داشته باشید و کوچکترین تغییری در آن ایجاد کنید، حال اگر بخواهید این تغییر در Router های دیگر نیز اعمال شود، تنها راهکار این است که بصورت دستی این تغییرات را در Router های دیگر وارد کنید و Routing Table آنها را بروز کنید.
اما با استفاده از پروتکل های Dynamic Routing دیگر نیازی نیست بصورت دستی Route ها را اضافه کنید، Router ها بصورت خودکار می توانند از Router های اطراف، تمامی اطلاعات مورد نیاز خود را برای انجام فرآیند Routing دریافت کنند.

فرآیند پیدا کردن بهترین مسیر در پروتکل های مسیریابی مختلف بصورت متفاوتی انجام می شود.
برخی از مسیریاب ها بسته به تعداد مسیریاب های بر سر راه، برای پیدا کردن مسیر بهتر استفاده می کنند و برخی فقط سریعترین مسیر را پیدا می کنند.Router هایی که در یک شبکه وجود دارند و از یک پروتکل مسیریابی Dynamic استفاده می کنند، اطلاعات موجود در Routing Tableهای خود را با همدیگر به اشتراک می گذارند تا همیشه بروز باشند.

در مسیریابیِ Dynamic، با استفاده از Routing Protocol ها این قابلیت بوجود می آید که Router ها مدام با شبکه تبادل اطلاعات داشته باشند و وضعیت هر یک از Router های دیگر را بررسی کنند و با استفاده از Broadcast یا Multicast با هم ارتباط برقرار کنند و اطلاعات Routing Table را بروز کنند.
با این روش همیشه توپولوژی شبکه به روز بوده و همه ی دستگاه های Router شبکه، از آخرین Routing Table به روز استفاده می کنند.

بطورکلی پروتکل های Dynamic دو دسته هستند:

IGPS (interior Gateway Protocols): که خودش شامل دو دسته می باشد:

❖ Distance Vector (بردار مسافت):

- پروتکل های Distance Vector از معیار Hop Count یا تعداد Router های حاضر در مسیر برای update جدول های مسیریابی خود استفاده می کنند.
- الگوریتم اینگونه پروتکل ها بسیار ساده است و Routing Table با محاسبات ساده ی ریاضی ایجاد می شود.
- پروتکل های Distance Vector معمولا برای شبکه های کوچکی که کمتر از 16 عدد Router در آنها وجود دارد، استفاده می شوند.
- در واقع این نوع پروتکل با کم کردن تعداد Router های مسیر، از به وجود آمدن Loop در شبکه یا Routing Loop در شبکه جلوگیری می کنند.
- این پروتکل ها در بازه های زمانی معین Routing Table های خود را با هم یکسان سازی می کنند.
- یکی از مشکلات الگوریتم های Distance Vector در این است که کلیه اطلاعات موجود در Routing Table خود را حتی با کوچکترین تغییر، برای سایر Router های مجموعه ارسال می کنند و در واقع Incremental Update را پشتیبانی نمی کنند که در نسخه های جدید الگوریتم های Distance Vector این مشکل حل شده است.

دو نوع از الگوریتم های Distance Vector :

➢ RIP (Routing Information Protocol): که نسخه ی یک آن منسوخ شده، و فقط v2 آن موجود است.
  - یکی از ساده ترین و قدیمی ترین پروتکل های مسیریابی در Router هاست.
  - برای شبکه های کوچک تا متوسط استفاده می شود.

➢ IGRP (Interior Gateway Routing Protocol):

❖ Link-State :

- الگوریتم های مورد استفاده در این نوع پروتکل ها نسبت به Distance Vector ها کاملا متفاوت عمل کرده و دارای پیچیدگی های خاص خود می باشند.
- در این الگوریتم ها از فاکتورهایی مثل Hop Count ، فاصله ، سرعت لینک و ترافیک بصورت همزمان برای تعیین بهترین مسیر استفاده می شود.
- آنها از الگوریتمی به نام Dijkstra برای تعیین پایینترین cost برای Route ها استفاده می کنند.
- روترهایی که از پروتکل های Link State استفاده می کنند فقط زمانی Routing Table های همدیگر را یکسان سازی می کنند که چیز جدیدی به Routing Table یکی از Router ها اضافه شده باشد؛ به همین دلیل کمترین ترافیک را در هنگام یکسان سازی Routing Table با یکدیگر ایجاد می کنند.

دو نوع از الگوریتم های Link State:

➢ OSPF (Open Shortest Path First):
  - این پروتکل همیشه به دنبال سریعترین مسیر برای رسیدن به مقصد می گردد.
  - Router هایی که در یک شبکه ی OSPF قرار دارند، همیشه وضعیت سایر Router هایی که به آنها دسترسی دارند را بررسی می کنند و هر زمان که لازم باشد برای همدیگر پیام می فرستند.
  - با استفاده از این مکانیزم Router ها وضعیت سایر روترهای موجود در شبکه را متوجه می شوند و می فهمند که آیا یک Router روشن است یا خیر.

- در OSPF، Router ها از سریعترین و نزدیکترین مسیر برای رسیدن به مقصد باخبر می شوند.در چنین حالتی قابلیت پیاده سازی Load Balancing در Router ها وجود دارد.به این صورت که بسته های اطلاعاتی را می توان به قطعات مختلف تقسیم کرده و در مسیرهای مختلفی به سمت مقصد ارسال کرد.
- OSPF را معمولا در شبکه هایی با ابعاد متوسط رو به بزرگ (large Network) استفاده می کنند و معمولا در شبکه های خیلی خیلی بزرگ، از این پروتکل کمتر استفاده می شود!
- الگوریتم OSPF در ویندوز سرور 2016 قابل پیاده سازی نیست!

➢ IS-IS (Intermediate System to Intermediate System):

EGPS (Exterior Gateway Protocols): که شامل یک الگوریتم می باشد:

❖ BGP (Border Gateway Protocol):

- در شبکه هایی استفاده می شود که واقعا کلان و بسیار بزرگ (extra large Network) هستند.
- مثلاً شبکه ای مثل اینترنت از پروتکل مسیریابی BGP استفاده می کند.
- این الگوریتم در شرکت های ارائه دهنده ی اینترنت (ISP ها) و یا شرکت هایی که با Cloud کار می کنند، استفاده می شود.
- البته می توان از BGP در شبکه های داخلی نیز استفاده کرد.
- الگوریتم BGP در ویندوز سرور 2016 قابل پیاده سازی است!
- برای ارتباطات S2S-VPN خیلی مفید واقع می شود.
- مسیریاب‌های BGP باید حافظه بسیار بزرگی و پردازه بسیار قدرتمندی داشته باشد.

Routing Service :

شبکه های با Subnet متفاوت، برای برقراری ارتباط با یکدیگر، درخواست خود را به Router ارسال می کنند و Router توسط لیستی از آدرس های IP که به آن Routing Table می گویند، به شناسایی مقصد درخواستهای ارسالی می پردازد.
درحقیقت برای برقراری ارتباط شبکه ها در سطح گسترده، از Router های فیزیکی استفاده می شود، اما برای ایجاد ارتباط میان دو یا چند شبکه در سطح محدود، می توان از قابلیت Routing موجود در ویندوز Server استفاده کرد.

در ساده ترین حالت، فرض کنید بخواهیم دو Server که آدرس های IP آنها در دو Range مختلف هستند را به یکدیگر متصل کنیم.
می توانیم به راحتی سرویس Routing را برای یکی از آنها پیکربندی کنیم، طوری که به عنوان یک Router در شبکه کار کند.
نکته: چون قصد داریم حداقل دو شبکه را به یکدیگر متصل کنیم، Server موردنظر باید حداقل 2 کارت شبکه داشته باشد.

در ابتدا برای اینکه از وضعیت مسیرهای موجود در سیستم یا همان Routing Table مطلع شویم، می توانیم در PowerShell درج کنیم:

```
Get-NetRoute
```

و یا در cmd دستور route print را وارد کنیم:

1. **اولین بخشی که مشاهده می شود Interface list نام دارد که در آن interface های شبکه (کارت شبکه ها) را می بینیم.**
   - **کاربرد آن برای زمانی ست که یک NIC را به Routing Table اضافه یا از آن حذف می کنیم.**
   - **به این ترتیب می توان از تعداد کارت شبکه های اضافه یا حذف شده با خبر شد.**

2. **دومین بخش، IPv4 Route Table است که بیانگر مقصدهایی ست که ویندوز Server، ترافیک را به آنها هدایت می کند.**
   - **Network destination : وقتی یک Route ایجاد می کنیم، دارای یک آدرس شبکه ی مقصد نیز می باشد.**
   مثلاً آدرس Network آدرس 23.1.2.101، می شود: 23.1.2.0
   - **Netmask : آدرس Subnet مربوط به IP مقصد را مشخص می کند.**
   - **آدرس Subnet ارسال های Broadcast به صورت 255.255.255.255 می باشد.**
   - **آدرس Subnet ارسال به خود هم به صورت 255.255.255.255 می باشد.**
   - **آدرس Subnet ارسال به آدرس Network یک محدوده، مطابق با Class آن می باشد.**
   مثلاً برای آدرس 192.168.2.0 که در کلاس C است، به صورت 255.255.255.0 می باشد.
   - **Gateway : هر IP آدرسی که سیستم به کمک routing table قادر به شناسایی آن نباشد، برای gateway ارسال خواهد شد.**
   - **Interface : نشان دهنده ی IP کارت شبکه ای است که سیستم، درخواست routing را از طریق آن ارسال خواهد کرد.**
   (در اینجا تنها NIC ها را در برنمی گیرد بلکه شامل loopback ، Bluetooth، wi-fi و ... نیز می شود.)
   - **Metric: پارامتری است که هزینه ی مسیر را برای رسیدن به مقصد مورد نظر بیان می کند.**
   این هزینه بسته به نوع الگوریتم Routing متفاوت است.

برای مشاهده ی Routing Table در محیط گرافیکی، می توان وارد کنسول RRAS شده و در زیرمجموعه ی IPv4 بر روی عبارت Static Routes راست کلیک کرده و گزینه ی show IP routing table را انتخاب کرد.

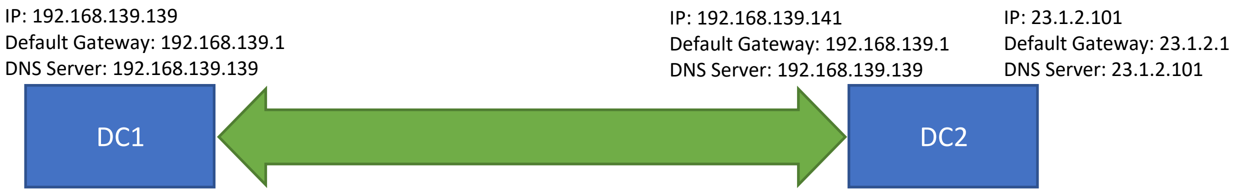
:BGP Router Implementation

فرض کنید دو Server زیر موجود هستند که می خواهیم آنها را تبدیل به BGP Router کنیم تا با یکدیگر یک ارتباط Neighborship برقرار کنند.

این ارتباط بر اساس یک شماره به نام ASN (Autonomous System Number) برقرار می شود که در هریک از دو طرف ارتباط باید تنظیم شود:

- اگر ASN در هردو Server یکسان باشد، پروتکل آنها Internal BGP یا IBGP خواهد شد.
- اگر ASN در Server ها متفاوت با یکدیگر باشند، پروتکل آنها External BGP یا EBGP خواهد شد.

نکته: در حقیقت DC2 دارای یک NIC برای شبکه ی داخلی خودش است، و یک NIC دیگر را برای اتصال به DC1 نیاز خواهد داشت.



1. کنسول RRAS را هم بر روی DC1 و هم DC2 راه اندازی می کنیم.

- در بخش Role Services، گزینه ی Routing را انتخاب می کنیم و تا پایان نصب پیش می رویم.
- از منوی Tools، وارد گزینه ی Routing and Remote Access می شویم.
- حال اگر در کادر سمت چپ این کنسول، آبجکت این Server موجود نبود، بر روی Routing and Remote Access کلیک راست و Add Server و سپس the Following Computer را زده و نام FQDN این سرور را درج و OK می کنیم.
- بر روی سرور اضافه شده، کلیک راست کرده و .Configure and enable Rout را می زنیم.
- گزینه ی Custom Configuration را انتخاب می کنیم.
- گزینه ی Lan Routing را انتخاب می کنیم و finish و Start Service را می زنیم.

2. تعیین می کنیم که Router کناریِ DC1 (همسایه) کدام است: پس وارد PowerShell می شویم.

- باید یک BGP Router را برای DC1 ایجاد کنیم، پس درج می کنیم:

```
Add-BgpRouter -BgpIdentifier 192.168.139.139 -LocalASN 65000
```

- مشخص می کنیم که این BGP Router به کدام BGP Router دیگر متصل می شود:

```
Add-BgpPeer -Name DC2 -LocalIPAddress 192.168.139.139 -PeerIPAddress 192.168.139.141 -LocalASN 65000 -PeerASN 65000
-PeeringMode Automatic
```

- برای Name می توانیم آدرس FQDN یا IP مقصد و یا NetBiosName آن را درج کنیم.

3. تعیین می کنیم که Router کناریِ DC2 (همسایه) کدام است: پس وارد PowerShell می شویم.

- باید یک BGP Router را برای DC2 ایجاد کنیم، پس درج می کنیم:

```
Add-BgpRouter -BgpIdentifier 192.168.139.141 -LocalASN 65000
```

- مشخص می کنیم که این BGP Router به کدام BGP Router دیگر متصل می شود:

```
Add-BgpPeer -Name DC2 -LocalIPAddress 192.168.139.141 -PeerIPAddress 192.168.139.139 -LocalASN 65000 -PeerASN 65000
-PeeringMode Automatic
```

4. در DC2 مسیر دسترسی به شبکه ی 23.1.2.0 را تعیین می کنیم (Advertise می کنیم):

- یعنی باید در DC2 برای DC های دیگر تعیین کنیم: برای دسترسی به شبکه ی 23.1.2.0 باید از DC2 گذشت (از خودش)
- در ابتدا اگر در هریک از DCها دستور زیر را وارد کنیم، احتمالاً می بینیم که هنوز هیچ مسیری برای پروتکل BGP وجود ندارد:

```
Get-BgpStatistics
```

- پس این Route را طوری تعریف می کنیم که توسط پروتکل BGP انجام شود.در PowerShell درج می کنیم:

```
Add-BgpCustomRoute -Network 23.1.2.0/24
```

- حال اگر در DC1 جدول Routing را فراخوانی کنیم، می بینیم که مسیری برای شبکه ی 23.1.2.0 ایجاد شده است.
- و اگر دوباره دستور statistics مربوط به bgp را بزنیم، می بینیم که یک مسیر برای IPv4 ایجاد شده است.
- و اگر دستور زیر و یا دستور Ping برای 23.1.2.101 را در DC1، امتحان کنیم، باید پاسخ مثبتی دریافت کنیم:

```
Test-NetConnection 23.1.2.101
```

Remove a Route:

- ابتدا نیاز به شماره ی InterfaceIndex آن Route داریم.پس درج می کنیم:

```
Get-NetRoute
```

- حال که در زیر ستون ifIndex این شماره را پیدا کردیم، (مثلاً 8) درج می کنیم:

```
Remove-NetRoute -InterfaceIndex 8 -DestinationPrefix 23.1.2.0/24
```

Virtualisation :

سالهاست که استفاده از ماشینهای مجازی (VM) و پیاده سازی انواع سرورهای مجازی (VS) روی یک سرور فیزیکی رواج پیدا کرده است. در حقیقت، در مجازی سازی، منابع فیزیکی-سخت‌افزاری بین همه ی سیستم های مجازی، به اشتراک گذاشته می‌شوند.

- در این حالت هر یک از سیستم‌های مجازی می‌توانند دارای سیستم‌عامل و نسخه ی کاملاً متفاوت از دیگران باشند.
- مثلاً یکی از سیستم‌ها به عنوان Domain Controller ایفای نقش می‌کند و تحت سیستم‌عامل ویندوز سرور ۲۰۱۲ است و دیگری با نسخه‌ای از سیستم عامل Linux به‌عنوان Cache Server عمل می‌کند.

استفاده از ماشین های مجازی و مشخصا سرورهای مجازی جهت کاهش تعداد سرورهای فیزیکی انجام می شود که خودش اهداف گوناگونی دارد:

- کاهش هزینه های مالی: دیگر احتیاج به خرید یک سرور فیزیکی به ازای هر سرویس نیست.
  می توان چندین سرویس را توسط یک سرور مجازی پیاده سازی کرد
- کاهش تعداد Rack های مورد استفاده جهت نگهداری سرورهای فیزیکی
  که باعث کاهش فضای مورد نیاز جهت اتاق سرور و یا اتاق Data center می شود.
- آزاد شدن تعداد زیادی از پورتهای سوئیچ های شبکه
- کاهش میزان استفاده از برق و تجهیزات خنک سازی
- مدیریت ساده تر سرورها و سرویس ها
- استفاده ی حداکثر از توان و منابع سرورهای فیزیکی.

فرض کنید در گذشته سرویس WSUS به تنهایی روی یک سرور فیزیکی پیاده سازی می شد.
مقدار زیادی از توان CPU و RAM و هارد سرور بلا استفاده می ماند.

ماشین های مجازی، مستقل از سخت افزار یا سیستم عامل اولیه به فعالیت خود ادامه می دهند.

نکته:

CPU مربوط به سیستمی که قصد Virtualisation Implementation بر روی آنرا داریم، باید این قابلیت را پشتیبانی کند.

برای فعال سازی آن:

- در سیستم فیزیکی، ابتدا به Setup Setting رفته و آن را که معمولا تحت عنوانی مثل Virtualization Technology است، Enable می کنیم.
- در سیستم مجازی در نرم افزار Vmware، به بخش تنظیمات CPU آن Virtual Machine رفته و گزینه های virtualization را فعال می کنیم.

می توان روی هر ماشین مجازی، یک سرور Implementation کرد؛ و این Virtual Server درست مثل یک Physical server رفتار می کند؛ که این امکان، نیازمند قابلیتی به نام VT-x در CPU های Intel و یا AMD می باشد.

به‌طور Example، یکی از سیستم‌ها به‌عنوان Domain Controller و تحت سیستم‌عامل Windows Server 2012 ایفای نقش می‌کند و دیگری با نسخه‌ای از سیستم عامل Linux به‌عنوان Cache Server عمل می‌کند.

هر ماشین مجازی به صورت کامل ایزوله و مجازی شده است و تفاوتی با یک سیستم فیزیکی ندارد.

Hypervisor :

دراغلب سیستم های مجازی ساز، یک لایه ی جدا کننده به نام **Hypervisor** میان سیستم عامل میهمان (مجازی) و سخت افزار حائل می گردد.

کار **Hypervisor** ایجاد یک دید مستقل مجازی از سخت افزار یا منابع است.

Hypervisor ها باعث می شوند ماشین های مجازی از دید یکدیگر پنهان بمانند و هر ماشین مجازی تصور کند که تمام سخت افزار یا منابع لازم را در اختیار گرفته است.

در حقیقت اصطلاح **Hypervisor** به مفهوم نظارتگر قوی تر است.

از آنجاییکه **hyper** عنوانی قوی تر از **super** است، پس **Hypervisor** از **Supervisor** قوی تر بوده و به معنی نظارت بر یک ناظر دیگر است.

Hypervisor یا «ناظر ماشین مجازی» می تواند یک نرم‌افزار یا یک ثابت افزار **Firmware** و یا یک سخت‌افزار باشد که سرویس **VM** (**Virtual Machine**) را فرآهم و اجرا می کند.

از **Hypervisor** با عنوان دیگری هم نام برده می شود که **VMM** نام داشته و مخفف کلمات **Virtual Machine Manager** و یا **Virtual Machine Monitor** می باشد.

هر رایانه‌ای که **Hypervisor** روی آن، یک یا چند ماشین مجازی را اجرا می کند، ماشین میزبان (**Host Computer**) و هر **Virtual Machine**، یک ماشین میهمان یا **Guest** نامیده می شود.

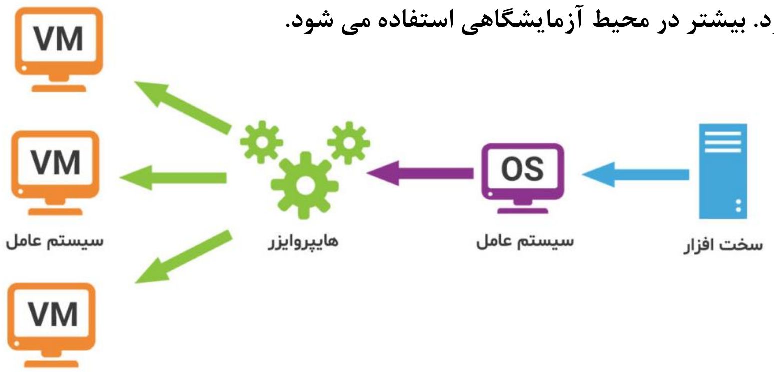
Hypervisor ها دو نوع هستند:

❖ Type 2 :

بر روی سیستم عامل میزبان نصب می شود و شما با استفاده از آن می توانید **OS** های خود را نصب و راه اندازی کنید.

به این نوع، **hosted hypervisor** هم گفته می شود. بیشتر در محیط آزمایشگاهی استفاده می شود.

از معایب آن این است که سرعت پایینی دارد.



نرم افزارهای زیر نمونه‌هایی از این نوع هستند:

- **VMware Workstation**
- **VMware Player**
- **VMware Fusion**
- **VirtualBox**
- **Parallels Desktop for Mac**
- **QEMU**

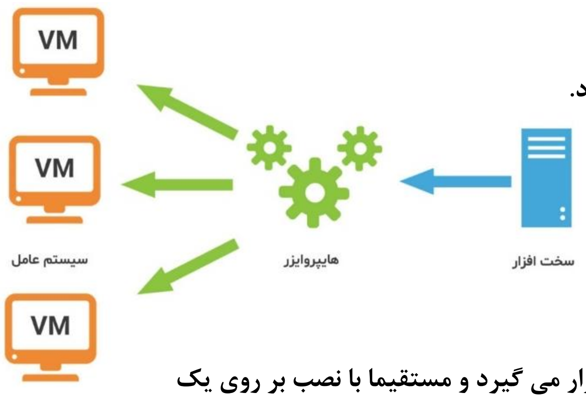
البته تشخیص تفاوت میان این دو نوع، زیاد واضح نیست، تنها می توان گفت که در نوع دوم، **Hypervisor** به شدت به **OS** میزبان وابسته بوده و اگر برای آن مشکلی بوجود بیاید، بر سایر سیستم عامل های مجازی میهمان هم بی تاثیر نخواهد بود.

❖ **Type 1 :**

سریع تر و قابل اطمینان تر از نوع دوم است.

به این دسته، **Native Hypervisor** یا **Bare Metal** نیز گفته می شود.

خود به دو دسته تقسیم می شود:



- **Monolithic Design** : به عنوان یک پلت فورم در اختیار شما قرار می گیرد و مستقیما با نصب بر روی یک سخت افزار **server** ، امکان نصب و راه اندازی تعدادی سیستم عامل مجازی دیگر را می دهد.
  در واقع در این نوع، خود **Hypervisor** نوعی سیستم عامل محسوب می شود.
  نرم افزار **ESXi** از شرکت **VMware** و نرم افزار **Xen** از شرکت **Citrix** از این دسته هستند.

- **Microkernelized Design** : از لحاظ ظاهری کاملاً مشابه با **Type 2** می باشد، در حالی که در زیرساخت سیستم، کاملاً مشابه با **Monolithic Design** عمل می کند.
  ❖ **Hyper-V** از این نوع می باشد.

نکته:

هنگام استفاده از نرم افزار های مجازی سازی، باید ویژگی مربوط به مجازی سازی CPU را در صفحه ی UEFI/Bios فعال کنیم که به یکی از نام های زیر قابل دسترسی است:

- **Intel VT-x**
- **AMD-V**
- **Intel-V**
- **SVM Support**
- **V-Support**
- **Virtualization Technology**
- **Intel Virtualization Technology**
- **Virtualization Extensions**
- **Vanderpool**
- **Virtual machin mode**
- **Virtualization Extensions**

Hyper-V :

اولین نسخه ی Hyper-V در Windows Server 2008 ارائه شد.
با معرفی ویندوز Server 2012، شاهد اولین نسخه ی Hyper-V بودیم که امکانات فوق العاده ای را به همراه داشت.
مدیریت Hyper-V به دوطریق ممکن است:

- **کنسول گرافیکی یا همان GUI**
- **کنسول دستوری PowerShell**

با قابلیت هایی که در Hyper-V وجود دارد، قادر خواهیم بود که قابلیت Online بودن یا همان Availability را به حداکثر برسانیم، بدون اینکه حتی لحظه ای خللی ایجاد شود.

معایت Hyper-V:

- **برخی از ویژگی های پیشرفته ی VMware را ندارد.**
- **فقط با سخت افزار 64 بیتی کار می کند.**

در حقیقت Hyper-V یک Hypervisor از نوع یک است. در صورتی که بطورظاهری مشابه با Hypervisor های نوع یک به نظر می رسد. اما پس از نصب آن بر روی ویندوز Server و یکبار Restart، بلافاصله خود ویندوز Server هم در زیرساخت سیستم، تبدیل به یکی از VM های زیرمجموعه ی HyperV خواهد شد، که در ظاهر اینطور به نظر نمی رسد!

- **Hyper-V اقدام به ایجاد Partition هایی به نام Virtual Hard Disk می کند.**
- **هر پارتیشن در واقع یک VM است و سخت افزار اختصاصی خود را دارد.**
- **نخستین پارتیشن بصورت خودکار و به محض نصب Hyper-v ایجاد می شود و Parent Partition نام دارد. (Host OS)**
- **سایر پارتیشنها بصورت دستی توسط مدیر شبکه ایجاد می شوند و Child Partition نام دارند.**
- **Parent Partition بر خلاف Child Partition ها به سخت افزار، دسترسی مستقیم دارد.**
- **در نتیجه Parent Partition به نوعی مسئول مدیریت امور سخت افزاری Child Partition هاست.**

فرض کنید واحد مالی، از یک نرم افزار حسابداری استفاده می کند که دارای قفل سخت افزاری می باشد.
قفل فوق در واقع یک USB Flash Disk است که باید به پورت USB ماشین host متصل شده و توسط سیستم عامل Child Partition شناسایی شود.
مدیریت این فرآیند، توسط Parent Partition صورت می پذیرد.

:Hyper-V Setup

نکته: از قبل از آن باید قابلیت مجازی سازی یا Vitualization را بر روی سیستم موردنظر، در تنظیمات BIOS، فعال کرده باشیم.

برای اطلاع از فعال بودن این قابلیت، در PowerShell، یکی از دو دستور زیر را درج می کنیم:

Systeminfo

```
Get-ComputerInfo
```

در پاسخ Systeminfo، در آخرین خط، باید در مقابل Hyper-V Requirements عبارت has been detected درج شده باشد.

در پاسخ Get-ComputerInfo، باید در مقابل HyperVisorPresent کلمه ی True درج شده باشد.

روی Windows 10 / 11:

اگرچه کاربرد حرفه ای تر Hyper-V، بر روی Windows Server است، اما می توانیم آن را بر روی Windows های معمولی هم راه اندازی کنیم.

1. **خط فرمان RUN را باز کرده و وارد appwiz.cpl شده و روی Turn Windows features on or off کلیک می کنیم.**
2. **در لیست ظاهرشده، گزینه ی Hyper-V و همه ی زیرگزینه های آن را فعال کرده و OK می کنیم.**
   نصب آغاز خواهد شد و سپس سیستم نیاز به یکبار restart خواهد داشت.
3. **پس از restart، به سادگی می توان در Start menu، گزینه ی Hyper-V Manager و یا هر عبارتی مشابه Virtual را جستجو کرد.**

روی Windows Server:

در حقیقت، HyperV یکی از نقش ها یا Role هایی است که در AD وجود دارد.

برای نصب Role آن، در پنجره ی Server Manager :

Manage > Add Roles and Features

- **اگر یک دیسک مجازی از قبل ایجاد کرده باشیم select a virtual HD را انتخاب می کنیم وگرنه که بدون تغییر Next!**
- **در پرده ی Server Roles گزینه ی Hyper-V را پیدا کرده و تیک آن را فعال کرده و next!**
- **در پرده ی virtual Switches باید کارت شبکه ای که قرار است Hyper-V با آن تماس برقرار کند را انتخاب کنیم که فعلاً انتخاب نمی کنیم.**
- **در پرده ی Confirmation تیک گزینه ی ...restart the destination server automa را فعال می کنیم، چون در میانه ی نصب Role مربوط به Hyper-V نیاز به Implementation مجدد خواهد بود.**

برای نصب آن همچنین می توانیم در PowerShell از دستور زیر استفاده می کنیم:

```
Install-WindowsFeature Hyper-v -IncludeAllSubFeature -IncludeManagementTools -Restart
```

نکته: برای دسترسی به کنسول گرافیکی HyperV در سیستم غیر Server که RSAT روی آن فعال است، باید در آن سیستم، وارد Programs and Features شده و به Turn Windows Features On or off رفته و از زیرگزینه های Hyper-V گزینه ی Hyper-V Management Tools را فعال کنیم و یکبار Restart! و یا در PowerShell درج کنیم:

```
Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V-Tools-All -All
```

نکته: برای نصب یک Feature یا Role بر روی یک VM، می توان در ماشین Host و در PowerShell هم این کار را انجام داد. اما باید برای آدرسِ آن، آدرس Virtual Disk آن را بدهیم. مثال:

```
Install-WindowsFeature web-server -Vhd F:\VHDs\VM1.vhdx
```

نکته: اگر خطا داد، باید آدرس را درون ' ' قرار دهیم.

: Virtual Switch

برای برقراری ارتباط میان Virtual Machine ها با شبکه ی واقعی، استفاده می شود که سه نوع دارد:

- External: مستقیماً امکان ارتباط میان VM ها با شبکه ی فیزیکی را برقرار می کند. این روش، کارت شبکه ی فیزیکی سیستم Host را به اعضای مجازی تخصیص می دهد.
  همه ی VM ها و Host و سوییچ فیزیکی، تحت آدرس IP سوییچ فیزیکی، با هم در ارتباط هستند.

- Internal : یک شبکه میان VM ها سیستم Host ایجاد می شود.
  همه ی VM ها و Host، تحت یک آدرس IP درون HyperV، با هم در ارتباط هستند.

- Private : برای برقراری ارتباط میان VM ها با یکدیگر استفاده می شود، طوری که Host هم به شبکه ی آنها دسترسی ندارد.
  همه ی VM ها، تحت یک آدرس IP درون HyperV، با هم در ارتباط هستند.

  بیشتر برای موارد آزمایش و تست و آموزشی بکار می رود.

برای ایجاد یا مدیریت Virtual Switch :

Tools > Hyper-V Manager> virtual switch manager

نوع مورد نظر را انتخاب و روی create virtual switch کلیک می کنیم.

یک نام درج می کنیم.

- اگر external باشد:
  - NIC فیزیکی مورد نظر را انتخاب می کنیم.
  - با فعال سازی گزینه ی **... allow management op** ، امکان به اشتراک گذاری این switch با فضای بیرون شبکه (مثلاً اینترنت) نیز فراهم می شود. (معمولاً آنرا فعال می کنیم.)
  - اگر NIC فیزیکی، قابلیت Single Root I/O را پشتیبانی کند، گزینه ی **...Enable Single roo** نیز موجود خواهد بود و می توان آن را فعال کرد.
    - در صورت فعال سازی آن، ارتباط این سوییچ با محیط بیرون، بطور مستقیم توسط NIC فیزیکی خواهد بود و نه تحت مدیریت سیستم Host!
    - وظیفه ی پردازش و مدیریت ترافیک بین این V-Switch و شبکه ی بیرون، به عهده ی خود NIC فیزیکی خواهد بود و نه CPU سیستم. که باعث افزایش سرعت خواهد بود.
  - می توان Vlan هم تعیین کرد.

ایجاد Switch توسط PowerShell :

```
New-VMSwitch -SwitchName InternSW -SwitchType Internal
```

نکته:

- به تعداد کارت شبکه های فیزیکی که بر روی سیستم Host نصب باشند، می تواند external Vswitch ایجاد کرد.
- پیشنهاد می شود که **حداقل دو NIC** فیزیکی بر روی HyperV Server نصب باشد:
  یکی برای ارتباطات بیرونی خود سیستم Host و یکی برای ارتباطات بیرون VM های HyperV.
- اگر از نوع internal باشد، تنظیم خاصی نیاز ندارد، فقط برای تشکیل شبکه های دقیق تر، می توان برای آن هم vLan ایجاد کرد.
- اگر از نوع private باشد هم تنظیم خاصی نیاز ندارد و این نوع VSW، نیازی به Vlan ندارد، پس این قابلیت برای آن غیرفعال است.

: Virtual Hard Disk

برای ایجاد یک Virtual Hard Disk :

از طریق GUI :

وارد کنسول HyperV شده و از منوی بالا و یا در سمت راست پنجره و در کادر Action :

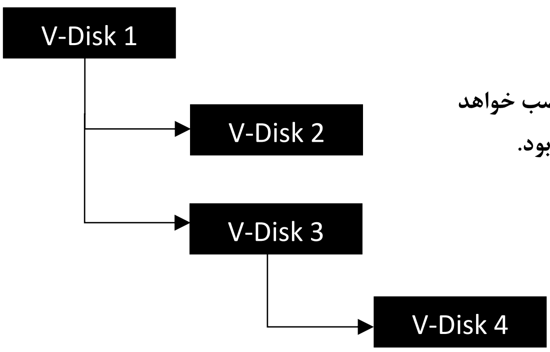
Action > new> Hard disk

حافظه های مجازی می توانند یکی از سه فرمت زیر را داشته باشند:

- **VHD** : فقط ویندوز های تا قبل از 8 و سرور 2012 و تا حجم حدود 2 Tera Byte را پشتیبانی می کند.
- **VHDX**: فقط ویندوز های از بعد از 8 و سرور 2012 و تا حجم حدود 64 Tera Byte را پشتیبانی می کند.
- **VHD Set** : برای حافظه های مجازی اشتراکی بکار می رود.

به سه شکل می توان به VHD، فضای مورد نظر را اختصاص داد:

- **Fixed Size** : به طور یکجا، یک حجم مشخص را از حافظه ی فیزیکی کسر و به حافظه ی مجازی اختصاصی دهد.
- **Dynamically expanding** : میزان فضای قابل اختصاص را دریافت می کند، اما فقط به میزان حجم داده های موجود در حافظه ی مجازی، از حافظه ی فیزیکی حجم دریافت می کند، تا زمانی که به سقف مشخص شده برسد.
- **Differencing** : زمانی که بخواهیم به شکل فوری یک ماشین مجازی ایجاد کنیم، این نوع VHD را انتخاب می کنیم.
  - در این حالت، هر VDisk جدید، به عنوان یک Child-VDisk برای سیستم بالادستی اش خواهد بود.
  - Child-VDisk ها، سیستم عامل و فضای مورد نیازشان را از Parent-VDisk دریافت می کنند.
  - نمی توان یک Disk تنها را از نوع Differencing ایجاد کرد، چون نیاز به Parent خواهد داشت.
  - اولین Parent، از یکی از دو نوع Fixed یا Dynamic هستند.



- فرض کنید بر روی Disk1، ویندوز Server نصب است.
- پس در Disk2 و Disk3 نیز، همان ویندوز Server با تنظیمات روی Disk1 نصب خواهد بود. اما هرتغییری که در Disk های دو و سه اعمال کنیم، فقط در آنها خواهد بود.
- در Disk4، تمام تنظیمات Disk1 و Disk3 تنظیم خواهد بود.

اگر Fixed یا Dinamically را بزنیم:

در پرده ی configure Disk می توانیم تعیین کنیم که:

- یک بخش مشخص از فضای دیسک یا دیسک های فیزیکی متصل به سیستم،
- یکی از دیسک های فیزیکی متصل به سیستم به طورکامل،
- یک دیسک مجازی که از قبل وجود داشته است،

را به آن اختصاص دهیم و تمام؛ و یا بطور کل در **PowerShell**:

```
New-VHD -Path F:\vhd1.vhdx -SizeBytes 50GB -Dynamic
```

اگر Differencing را بزنیم:

در پرده ی configure Disk، باید Parent Disk را مشخص کنیم و تمام؛ و یا بطور کل در **PowerShell**:

```
New-VHD -Path f:\Disk\Diff.vhdx -ParentPath f:\Disk\VM1.vhdx -Differencing
```

- برای متصل کردن یک حافظه ی مجازی به یک ماشین مجازی:

```
Add-VMHardDiskDrive -VMName vm1 -Path F:\vhd1.vhdx -ControllerType SCSI -ControllerNumber 0 -ControllerLocation 3
```

برای مشاهده ی مشخصات یک Virtual Hard Disk :

از منوی بالا و یا در سمت راست پنجره:

Action > Inspect Disk

مشکل Differencing Disk ها:

- وقتی VM صاحب Parent Disk روشن است، نمی توان از آن Child Disk ایجاد کرد.
- وقتی یک Differencing Disk روشن است، نمی توان یک Differencing Disk دیگر متصل به آنرا (Parent / Child) روشن کرد.
- گاهی ممکن است هنگام روشن کردن یک VM که دارای یک Differencing Child Disk است، با خطای اتصال به Parent Disk مواجه شویم و روشن نشود.
  این به دلیل ایجاد یک تغییر در Parent Disk می باشد. مثلاً نصب و راه اندازی یک Feature و یا ... .
  برای رفع این مشکل، باید به VM Setting رفته و virtual Disk را انتخاب و Inspect را بزنیم.
  - اگر پنجره ی Inspect باز شد:
    خطای قطع ارتباط را می بینیم. پس دکمه ی Reconnect را می زنیم و در Wizard باز شده، برای Parent Disk، به آدرس Parent Disk رفته و آن را انتخاب کرده و در زیر آن، دکمه ی Ignore ID mismatch را می زنیم و next و تمام!
  - اگر پنجره ی Inspect باز نشد:
    دکمه ی Edit را می زنیم و و در Wizard باز شده، برای Parent Disk، به آدرس Parent Disk رفته و آن را انتخاب کرده و در زیر آن، دکمه ی Ignore ID mismatch را می زنیم و next و تمام!

- راهکار بهتر است که Parent VM را از VM ای که در آن قرار دارد هم جدا کرده و استفاده نکنیم، و به جای آن، دوباره از Parent یک Child تهیه کنیم و در VM ای که در آن بوده، استفاده کنیم.

برای ویرایش یک Virtual Hard Disk :

از منوی بالا و یا در سمت راست پنجره:

Action > Edit Disk

پس از انتخاب فایل Virtual Hard Disk:

- **Compact** : فضای خالی ایجاد شده بر اثر حذف فایلها بر روی یک VHD را حذف می کند؛ به عبارتی آزاد می کند.

```
Optimize-VHD -Path F:\VHDs\vhd3.vhdx
```

- **Convert** : برای تبدیل یک Virtual Disk به فرمت های دیگر استفاده می شود.(Dynamic, Fixed و ...)

```
Convert-VHD -Path F:\VHDs\vhd3.vhdx -DestinationPath F:\VHDs\vhd3-1.vhdx -VHDType Fixed -DeleteSource
```

نکته: در حقیقت سوییچ DeleteSource، فایل قبلی را حذف می کند.

- **Expand** : برای افزایش فضای VHD استفاده می شود. البته توسط دستور زیر، بطور کل می توان حجم را تغییر داد:

```
Resize-VHD -Path F:\VHDs\vhd3.vhdx -SizeBytes 54GB
```

- اگر فضای Disk از نوع Differencing باشد، در اینجا یک امکان دیگر موجود خواهد بود:
  Merge : برای ادغام کردن یک Child-Disk با یکی از گزینه های زیر استفاده می شود:
  - با Parent Disk خودش،
  - و یا با درج یک نام و پسوند .vhdx آن Differencing Disk را در قالب یک Disk مجزا ذخیره می کند.

```
Merge-VHD -Path F:\VHDs\vhd3.vhdx -DestinationPath F:\VHDs\vhd2.vhdx
```

: Virtual Machine

برای ایجاد ماشین مجازی:

از طریق GUI :

وارد کنسول HyperV شده و از منوی بالا و یا در سمت راست پنجره و در کادر Action :

New > Virtual Machine

- یک نام و در صورت نیاز، یک محل ذخیره سازی دلخواه، برای آن تعیین می کنیم.
- دو نوع نسل یا Generation برای یک VM می توان انتخاب کرد.
  - : Generation 1
    - فقط سیستم های 32 و 64 بیتی را پشتیبانی می کند.
    - برای ویندوزهای 7 و 8 و Server 2008 و برخی نسخه های Linux این گزینه را انتخاب می کنیم.
    - Emulation Based است، یعنی بر اساس تقلید یا پیروی از سخت افزارهای موردنیاز یا درایورها.
    - DVD Rom را بر اساس IDE تقلید یا emulate می کند.
    - Bios آن از نوع Legacy است.
  - : Generation 2
    - فقط ویندوز های از بعد از 8 و بعد از سرور 2012 و فقط سیستم های 64 بیتی را پشتیبانی می کند.
    - سرعت بالاتری دارد.
    - Emulation Based است، یعنی بر اساس تقلید یا پیروی از سخت افزارهای موردنیاز یا درایورها.
    - DVD Rom را بر اساس scsi تقلید یا emulate می کند.
    - Bios آن از نوع UEFI است.
- می توان مقدار 2048 مگابایت را برای مقدار RAM ماشین، تعیین کرد و گزینه ی Use dynamic memory را فعال کرد تا به مقدار مورد نیاز، از RAM سیستم استفاده کند و کمبود RAM در ماشین های مجازی نیازمندتر جبران شود.
- در قسمت Configure Networking، می توانیم یکی از Switch های مجازی که ایجاد کرده بودیم را برای آن انتخاب کنیم.
- برای اختصاص یک VHD سه گزینه وجود دارد:
  - یک نام و آدرس وارد کنیم و یک حافظه ی مجازی، در حین ایجاد ماشین مجازی، برای آن ایجاد کنیم.
  - آدرس یک VHD که از قبل ایجاد کرده بودیم را وارد کرده و به آن اختصاص دهیم.
  - می توانیم حافظه ای برای آن تنظیم نکنیم و آن را به بعداً موکول کنیم.
    - فرض کنید گزینه ی سوم را زدیم. پس از ایجاد VM، روی آن کلیک راست کرده و وارد Setting می شویم، و Add Hardware و سپس SCSI Controller و Add را زده و بعد Hard Drive را انتخاب و Add کرده و در صفحه ی بعد از طریق Browse ، فایل VHD مورد نظر را پیدا و انتخاب می کنیم.
- برای تب Installation Options، بهترین کار این است که:
  - یا گزینه ی Install an OS later را بزنیم و پس از ایجاد شدن آن، ابتدا یک DVD Rom ایجاد کرده و Image مربوط به ویندوز را به آن Attach کنیم.
  - و یا اگر WDS Server را فعال کرده ایم، گزینه ی Install an OS from a bootable image file را بزنیم.
- برای روشن کردن سیستم یک VM، کلیک راست کرده و Start را می زنیم.
- برای مشاهده ی وضعیت (Monitor) یک VM، کلیک راست کرده و Connect را می زنیم.

از طریق PowerShell :

```
new-vm -Name VM3 -MemoryStartupBytes 2GB -NewVHDPath F:\VHDs\vhd3.vhdx -NewVHDSizeBytes 40GB -Generation 2
```

- در PowerShell می توان بطورهمزمان چند VM را روشن و خاموش و Restart کرد و لیست و وضعیت آنها را دریافت کرد:

```
Start-VM -Name VM1,VM2
Get-VM
Restart-VM vm1
Stop-VM -Name VM1
```

Virtual DVD Drive و Booting:

از طریق GUI :

- روی VM ایجاد شده کلیک راست و Setting را می زنیم.
- برای تنظیم اولویت Boot سیستم:
- در Generation 1 در گزینه ی Bios ؛ و برای Gen.2 در گزینه ی Firmware.(با دکمه ی move up و move down)
- برای تنظیم یا ایجاد DVD Drive:
  - در Gen.1 یک DVD Drive در زیرمجموعه ی IDE Controller موجود خواهد بود.
  - در Gen.2، گزینه ی Add Hardware و سپس SCSI Controller و سپس Add.

DVD Drive را انتخاب کرده و اگر فایل مورد نظرمان بصورت فایل Image باشد، Image را فعال کرده و به آدرس آن رفته و انتخابش کرده و در پایان Ok.

از طریق PowerShell:

ابتدا یک SCSI Controller در VM ایجاد می کنیم:

```
Add-VMScsiController -VMName VM3
```

نکته:

- ✓ وقتی یک VM ایجاد می کنیم، بطورخودکار دارای یک SCSI Controller خواهد بود، پس شماره ی ControllerNumber آن برابر با صفر خواهد بود.
- ✓ به تعداد دلخواه می توان SCSI Controller ایجاد کرد، که به ترتیب دارای شماره های یک و دو و ... خواهند بود.
- ✓ هر SCSI Controller، تنها 64 درگاه یا Location می تواند داشته باشد.
- ✓ از طرف دیگر هر SCSI Controller دارای درگاه های اتصال یا Controller Location های زیادی می باشد.

حال یک DVD Drive اضافه و Image مربوط به نصب ویندوز را به آن متصل می کنیم:

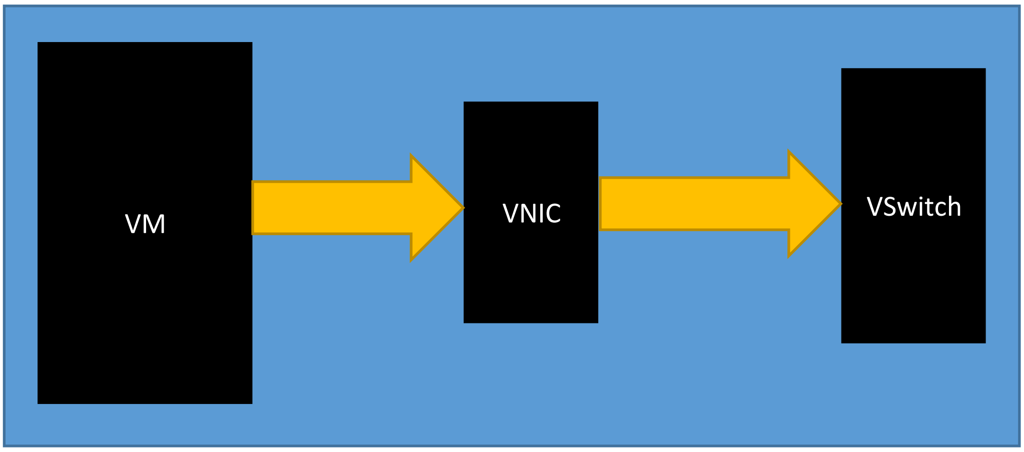
```
Add-VMDvdDrive -VMName VM3 -ControllerNumber 1 -ControllerLocation 0 -Path 'E:\SVR2016.iso'
```

❖ برای حذف یکی از Firmware ها ، مثلاً Network Adapter، از طریق PowerShell، دستورات زیر را به ترتیب وارد می کنیم:

```
$old = Get-VMFirmware -VMName vm1 | Select-Object -ExpandProperty BootOrder
$new = $old | Where-Object { $_.BootType -ne "Network" }
Set-VMFirmware -VMName vm1 -BootOrder $new
Get-VMFirmware -VMName vm1 | Select-Object -ExpandProperty BootOrder
```

: Virtual NIC

برای برقراری ارتباط میان Virtual Machine ها با Virtual Switch ها، نیاز است که هریک از VM ها، حداقل یک کارت شبکه ی مجازی یا VNIC هم داشته باشد.



پس در Setting یک VM وارد Add Hardware شده و سپس Network Adapter و Add .

نکته: اگر Generation 1 باشد، برای نصب ویندوز از طریق Boot PXE، باید گزینه ی Legacy Network Adapter را بزنیم.

در قسمت Virtual Switch، سوییچی که قصد اتصال به آن را داریم را انتخاب می کنیم و تمام!

البته می توان حداقل و حداکثر استفاده از پهنای باند شبکه و یک Vlan نیز برای این NIC تعیین کرد.

برای مشاهده ی تنظیمات و مشخصات کامل یک NIC متصل به یک VM، درج می کنیم:

```
Get-VMNetworkAdapter -VMName Name
```

نکته:

یکی از ویژگی هایی که به این طریق می توان مشاهده کرد، اما از طریق GUI نمی توان، Virtual Subnet ID می باشد.

نکته:

با توجه به اینکه MAC Address همه ی VM های یک HyperV Server، تا چند بخش اول، یکسان خواهند بود؛ می توانیم در DHCP Server شبکه، توسط قابلیت Filtering، یک Range از IP های یک Scope را به آنها اختصاص دهیم.

: VM Setting

: Security

- اگر توسط RSAT به HyperV متصل شده باشیم، این گزینه، در گزینه ی Firmware ادغام می شود.
- فعال کردن گزینه ی Enable Secure Boot مانع اجرای کدهای مخرب در هنگام اجرای VM می شود.
- برای نصب سیستم عامل های قدیمی Linux بر روی VM، نباید این گزینه را فعال کرد.
- اگر گزینه ی Microsoft Windows را انتخاب کنیم، فقط سیستم های ویندوزی را می توان روی VM نصب کرد.
- اگر Micrsft UEFI Certificate را بزنیم، می توان Linux های سطح بالا مثل Ubunto یا Cent OS را هم بدون مشکل نصب کرد.
- از طریق PowerShell :

```
Set-VMFirmware -VMName VM4 -EnableSecureBoot off
Set-VMFirmware -VMName VM4 -SecureBootTemplate microsoftueficertificate authority
```

: Memory

اگر سیستم عامل روی VM، ویندوز 10 یا Server 2016 باشد، برای تغییر مقدار Memory می توان در حالتی که VM روشن است این کار را انجام داد و تغییرات اعمال خواهند شد. اعدادی بین 512 ؛ 1024 ؛ 2048 ؛ 3072 ؛ 4096 ؛ 5120 ؛ 6144 ؛ 7168 و ...

```
Set-VMMemory -VMName vm4 -StartupBytes 3072MB
```

- با فعالسازی dynamic Memory ، می توان یک حداقل میزان استفاده (Shrinking) و یک حداکثر میزان استفاده (balloning) از RAM را برای VM تعیین کرد.

و یا توسط PowerShell همه ی آنها را تنظیم می کنیم:

```
Set-VM -Name VM1 -MemoryStartupBytes 2GB -DynamicMemory -MemoryMinimumBytes 1GB
-MemoryMaximumBytes 3GB
```

فرض کنید بخواهیم این تنظیمات را برای همه ی VM ها انجام دهیم:

```
Get-VM | Set-VM -MemoryStartupBytes 2GB -DynamicMemory -MemoryMinimumBytes 1GB -MemoryMaximumBytes 3GB
```

- می توان مقدار Buffer را برای VM تعیین کرد و توسط پارامتر Memory weight، میزان اولویت یک VM را برای دریافت سطح بیشتر یا کمتری از RAM تعیین کرد.

```
Set-VMMemory -VMName vm1 -Buffer 15 -Priority 50
```

- برای مشاهده ی مقادیر RAM در زمان اجرا، کافی ست در کنسول HyperV، آن VM را انتخاب کرده و در کادر پایین، وارد تب Memory شویم:

Assigned Memory : مقدار RAM اختصاص یا تعیین شده برای آن است.

Memory Demand : مقدار RAM موردنیاز در هر لحظه.

نکته: در حقیقت Host Provider ها، که Host را با یک سری مشخصات کرایه می دهند، گزینه ی dynamic را فعال نمی کنند.

: Network Adapter

- اگر برای Network Adapter، تیک گزینه ی .Enable virtual LAN identi را فعال کنیم، اتصالش با Host، که خود Parent Windows Server می باشد، قطع خواهد شد.

:Integration Services

همه ی گزینه های آن را فعال می کنیم.

برای مشاهده ی آنها در PowerShell:

```
Get-VMIntegrationService -VMName vm1
```

و فعال کردن یکی از آنها:

```
Enable-VMIntegrationService -VMName vm4 -Name "guest service interface"
```

Checkpoints :

به کمک این قابلیت می توان از حالت فعلی یک ماشین، یک **Snapshot** گرفت و در زمان بروز مشکل در نسخه فعلی، نسخه ی **Snapshot** را اجرا نمود.

دو نوع **Checkpoint** وجود دارد :

- **Standard Checkpoint:**

هنگامی که یک **Checkpoint** ایجاد می شود، شامل حالت فعلی **VM** و **Memory** آن و پیکربندی سخت افزارش است.

- **Production Checkpoint :**

هنگامی که یک **Checkpoint** ایجاد می شود، **Hyper-V** از سرویس **Volume Shadow** استفاده می کند تا حالت فعلی **VM** را به عنوان **Backup** بگیرد. در این حالت، **Memory** و پیکربندی سخت افزار، ذخیره نمی شوند.

در ویندوز ۱۰ و ویندوز سرور ۲۰۱۶، وقتی که یک **VM** جدید می سازیم، به صورت پیشفرض **Production Checkpoint** ایجاد خواهد شد.
اگر **VM** را از نسخه های قدیمی سیستم عامل **import** کنیم، به صورت پیشفرض **Standard** خواهد بود.

- با نگهداری زیاد و افزایش تعداد **Checkpoint** ها، سرعت و کارایی سیستم، خیلی کُند می شود.
- درصورت ایجاد مشکل و یا خراب شدن هارد اصلیِ **VM**، تمام **Checkpoint** ها بدون کاربرد می شوند. (از بین می روند).

- از **Standard Checkpoint** ها برای زمانی که بخواهیم چیزی را به سرعت تست و آزمایش کنیم، بسیار عالی و فوق العاده اند، که اگر مشکلی در سیستم و شبکه پیش بیاید، به راحتی **VM** را به حالت قبل باز می گردانیم.
- و از **Production Checkpoint** ها می توان برای محیط کار هم استفاده کرد.

Standard :

در تنظیمات **Checkpoint**، گزینه ی **Standard** را انتخاب کرده و **OK** می کنیم.

- بر روی **VM** کلیک راست کرده و **Checkpoint** را می زنیم، که اولین **Checkpoint** ایجاد شود.

برای بازگشت به یک **Checkpoint** بهتر است که نمای **Screen** را بسته باشیم.

- سپس در کادر **Checkpoints** در میانه ی کنسول **HyperV**، بر روی **Checkpoint** موردنظر کلیک راست کرده و **Apply** را می زنیم.

اگر وارد **Setting** مربوط به **VM** شویم، می بینیم که فرمت **Vdisk** ها به **.avhdx** تغییر کرده است.

- اگر بر روی هریک از **Checkpoint** ها کلیک راست کنیم، می توانیم توسط گزینه ی **Export**، آن وضعیت از **VM** را، ذخیره کنیم.

Production :

در تنظیمات **Checkpoint**، گزینه ی **Production** را انتخاب کرده و تیک **... Create Standard Checkpoints if** را برداشته و ذخیره می کنیم.

Set-VM -Name VM3 -CheckpointType ProductionOnly	فعالسازی و تنظیم **Checkpoint**
Checkpoint-VM -VMName vm3 -SnapshotName FirstCH	ایجاد یک **Checkpoint**
Get-VMSnapshot -VMName vm3	مشاهده ی همه ی **Checkpoint** ها
Restore-VMSnapshot -VMName vm3 -Name FirstCH	بازگشت به یک **checkpoint**
Get-VMSnapshot -VMName vm3 | Remove-VMSnapshot	حذف همه ی **Checkpoint** ها

نکته: پس از ایجاد دومین **Checkpoint**، دیگر به هیچ وجه نباید بر روی اولین **Checkpoint** تغییری ایجاد کرد.

: Smart Paging File Location

- آدرسی را در حافظه ی سیستم تعیین می کنیم که در صورت کمبود RAM برای اجرای VM، از آن به عنوان فضای مورد نیاز به عنوان RAM استفاده شود و پس از Restart و یا روشن شدن، کم کم میزان RAM ای که نیاز دارد را دریافت می کند.
- می توان پوشه ای به نام Paging را درون فایل مربوط به هر VM ایجاد کرد و برای هریک از آنها آدرس پوشه ی Paging را داد.
- برای راه اندازی این قابلیت، نیاز است که dynamic Memory در گزینه ی Memory غیرفعال باشد.

می توان توسط دستور زیر، آدرس PagingFile را برای همه ی VM ها یکسان تنظیم کرد:

```
Get-VM | Set-VM -SmartPagingFilePath f:\HiPage
```

: Automatic start action

برای تعیین چگونه روشن شدن و بکارافتادن VM پس از روشن شدن و ورود سیستم فیزیکی، بکار می رود، که سه حالت دارد:

- هیچ اتفاقی نیفتد، یعنی روشن نشود.
- بطور خودکار اجرا شود، اگر در آخرین بار در حال اجرا بوده است و سرویس ناگهان قطع شده بود.
- همیشه پس از روشن شدن سیستم فیزیکی، این VM بطور خودکار اجرا شود.

که البته می توان یک مقدار تأخیر بین روشن شدن سیستم فیزیکی و اجرای VM هم تعیین کرد.

: Automatic Stop Action

برای تعیین حالت VM در صورت ناگهانی خاموش شدن سیستم فیزیکی، بکار می رود.

VM Upgrade :

همانطور که می دانیم در هریک از نسخه های **Windows Server**، یک ورژن از **HyperV** هم موجود است. حال اگر بخواهیم یک **VM** را از نسخه های قدیمی تر به ویندوز **Server** با نسخه ای جدیدتر انتقال دهیم، باید آن را **Update** کنیم که بتواند از همه ی امکانات نسخه ی **HyperV** استفاده کند.

برای مشاهده ی ورژن یک **VM**، آن را انتخاب کرده و در کادر پایین، در تب **Summary** در مقابل **Configuration Version**.
اما هر **VM**، نسخه های مختلفی را **Support** می کند که در مقابل این گزینه، نسخه ای را نشان می دهد که فعلاً بر روی آن تنظیم است.

برای مشاهده ی همه ی نسخه های قابل پشتیبانی یک **VM** :

```
Get-VMHostSupportedVersion
```

پس اگر یک **VM** را از نسخه های قدیمی به نسخه ای جدید از **HyperV** وارد کردیم، برای **Update** آن:

```
Update-VMVersion -VM VM1
```

Shared Drive :

Shared Drive یک **Virtual Disk** است که بین یک سری **VM** به اشتراک گذاشته خواهد شد و همگی به سادگی به محتویات آن دسترسی خواهند داشت.

دو نوع دارد:

- **VHDx** : در حقیقت، نوعی **V Disk** است با تمام قابلیت ها و ویژگی های آنها، به جز موارد زیر، که فاقد آنهاست:
  Resize ؛ **Migrate** ؛ **Backup** ؛ **Replicate**
  در نتیجه کارآیی آنچنانی نخواهد داشت.

- **VHD Set** : تمام ناتوانی های گزینه ی اول را قادر به اجراست؛ و شامل دو فایل است:
  VHDs : یک **meta Data** ست که **260MB** حجم دارد.
  AVHDx : فایل اصلی **shared virtual Disk** است.

- تمامی **VM** هایی که به این **Virtual Shared Disk** متصل می شوند، جزیی از یک **Failover Cluster** خواهند بود.
- به این شکل که همه ی آنها، دارای یک نقش یکسان هستند، و اگر یکی از آنها از کار بیفتد، دیگری وظایف را ادامه می دهد.

- یک **SCSI Controller** را انتخاب کرده و گزینه ی **Shared Drive** را انتخاب و **Add** و سپس **New** را می زنیم.
- **VHD Set** را انتخاب و سپس می توان **Danamically** را انتخاب کرد.
- یک نام و یک آدرس ذخیره سازی برای آن تعیین می کنیم. (پسوند آن **vhds** است)
- یک حجم را اختصاص داده و تمام!
- حال باید آن را عضو یک **Cluster** کنیم.

و یا از طریق **PowerShell** :

```
New-VHD -Path f:\Disk\ShareDisk.vhds -SizeBytes 60GB -Dynamic
```

:Join a Physical Disk

گاهی نیاز است که یک **Disk** فیزیکی را کاملاً به یک **VM** اختصاص دهیم، که این کار توسط قابلیتی به نام **Pass-through** انجام می شود.
اگرچه، محدودیت هایی هم در پی خواهد داشت، مثل عدم **Backup** و عدم **Migration**.

- ابتدا باید **Disk** را آماده کنیم، پس آن را به صورت فیزیکی متصل می کنیم و **initialize** و سپس **Offline** می کنیم.
- به **VM Setting** موردنظر رفته و یک **SCSI Controller** را انتخاب کرده و یا یکی جدید ایجاد کرده و گزینه ی **Hard Disk** را می زنیم.
- گزینه ی **Physical Disk** را انتخاب و دیسک اضافه شده را نیز انتخاب کرده و **Ok** و تمام!

و یا از طریق PowerShell :

```
Add-VMScsiController -VMName VM1

Add-VMHardDiskDrive -VMName VM1 -DiskNumber 2 -ControllerType SCSI -ControllerNumber 1 -ControllerLocation 0
```

: Hyper-V Setting

در کادر سمت چپ کنسول Hyper-V، بر روی آبجکت Server جاری، کلیک راست کرده و Hyper-V Setting را می زنیم.

❖ Virtual Hard Disks :

در Virtual Hard Disk و در Virtual Machines می توان مکان پیشفرض ذخیره سازیِ VHD ها و خود VM ها را تعیین کرد.

و از طریق PowerShell هم می توان:

```
Set-VMHost -VirtualHardDiskPath f:\VHDS -VirtualMachinePath F:\VHDS
```

❖ NUMA (Non-uniform Memory Access):

همانطور که می دانیم، هر CPU نیاز به مقداری RAM دارد.

وقتی یک PC یا یک VM نیاز زیادی به پردازش های زیادی داشته باشد، می توان برای آن دو یا چند CPU نصب کرد.

در نتیجه، به هر CPU مقداری RAM تعلق خواهد گرفت که به ترکیب این دو قطعه، یک Node گفته می شود.

اگر قابلیت NUMA را برای آن سیستم یا VM فعال کنیم، در صورتی که مقدار RAM مربوط به یکی از CPU ها کم و ناکافی باشد، آن CPU می تواند از RAM مربوط به Node دیگر استفاده کند.

به طورمعمول Server های SQL Server نیاز به فعالسازی NUMA خواهند داشت.

برای فعال سازی آن در HyperV:

- درون HyperV Settings وارد گزینه ی NUMA Spanning شده و آن را فعال می کنیم. و یا:

```
Set-VMHost -NumaSpanningEnabled $true
```

- سپس به VM Setting موردنظر رفته و در زیرمجموعه های Prossesor وارد NUMA شده و تنظیمات را تعیین می کنیم و یا یکبار دکمه ی Use Hardware Topology را زده تا طبق تنظیمات سخت افزاری و خودکار تنظیم شوند.

❖ Resource Metering :

برای نظارت کردن بر میزان استفاده ی VM ها از منابع Host، از این قابلیت استفاده می کنیم که برای فعال سازی آن از دستور زیر استفاده می کنیم:

```
Get-VM | Enable-VMResourceMetering
```

برای بررسی اینکه این قابلیت بر روی VM ها فعال است یا خیر:

```
Get-VM | fl name, *res*
```

حال برای نظارت یا monitor کردن به کمک Resource metering :

```
Get-VM | Measure-VM
```

برای غیرفعالسازی آن:

```
Get-VM | Disable-VMResourceMetering
```

❖ Enhanced Session Mode Policy:

➢ تیک آن را فعال کرده و سپس به گزینه ی **Enhanced Session Mode** رفته و آن را نیز فعال می کنیم و **OK**!

```
Set-VMHost -EnableEnhancedSessionMode $true
```

➢ حال وارد **VM Setting** مربوط به **VM** موردنظر رفته و در گزینه ی **Integration Services**، همه ی گزینه های سمت راست را تیک می زنیم. (**Guest Services**)

نکته: برای کارکرد صحیح این قابلیت، باید سرویس **Remote desktop services** در کنسول **Services** درون **VM**، فعال و **Run** باشد.

- با فعال کردن این گزینه، در **VM**ها، به یک سری از منابع سیستم **Host** می توان بطور مستقیم دسترسی داشت. مثل: پرینتر، درگاه های **USB**، خروجی های صدا و درایوهای حافظه ی **Host**.
- می توان **Resolution** مربوط به **Display** هریک از **VM** ها را تعیین کرد.

➢ سپس باید یکبار **VM** موردنظر را خاموش و روشن کرد.

➢ پس از راه اندازی مجدد، فوراً با پنجره ی تنظیمات مواجه می شویم:
  - می توان **Display Size** را تنظیم کرد.
  - اگر **Show Options** را زده و وارد تب **Local Resources** شویم:
    - می توان بلندگو و میکروفون **Host** را به آن متصل کرد.
    - می توان درایوهای حافظه ی **Host** را با آن اشتراک گذاری کرد.

➢ اگر تیک گزینه ی **Save my settings for future...** را بزنیم، این پنجره دیگر ظاهر نشده و تنظیمات اعمال شده، ثابت می مانند.

➢ اما اگر بعدها بخواهیم این تنظیمات را تغییر دهیم، و نیاز به این پنجره داشته باشیم، در **PowerShell** درج می کنیم:

```
VMConnect.exe Host-ComputerName VM-Name /edit
VMConnect.exe IFM VM1 /edit
```

- در پنجره ی نمایش وضعیت **VM**، برای بازگشت به حالت قبل، در ابزار بالا، بر روی **Basic Session** می زنیم.

: Nested Virtualization

توسط این قابلیت، می توان خودِ یک **Virtual Machine** درون **HyperV** را (که دارای **Windows Server** است) تبدیل به یک **Host Machine** کرد. (**Host Virtual Machine**)

1. ابتدا توسط دستور زیر، قابلیت **HyperV** را درون آن **VM** نصب می کنیم:

```
Install-WindowsFeature Hyper-V -IncludeAllSubFeature -IncludeManagementTools -Restart
```

نکته: احتمالاً خطایی مبنی بر اینکه **Processor**، قابلیت مجازی سازی را پشتیبانی نمی کند، را می دهد.

❖ برای فعال سازی این قابلیت برای یک **VM**، ابتدا آن **VM** را خاموش کرده و در **PowerShell** درج می کنیم:

```
Set-VMProcessor -VMName VM1 -ExposeVirtualizationExtensions $true
```

: Virtual VLAN

VLAN ها را هم می توان بر روی VSwitch ها و هم بر روی VM ها پیاده سازی کنیم.

برای VSwitch:

- وارد تنظیمات Virtual external Switch شده و گزینه ی VLAN را فعال کرده و برای VLAN ID یک عدد درج می کنیم. مثلاً:205
- حال برای اتصال این Switch به هر سوییچ دیگری در شبکه، باید همین VLAN ID را درج کنیم.
- البته برای اتصال آن به سوییچ فیزیکی، باید علاوه بر درج این VLAN ID، قابلیت trunking را نیز فعال کنیم.

برای VM:

- باید ابتدا آن را turn off کرد.
- سپس وارد تنظیمات VM شده و گزینه ی Network Adapter را انتخاب کرده و گزینه ی VLAN را Enable کرده و برای VLAN ID یک عدد درج می کنیم.

: Virtual MAC Address

در HyperV می توان مجموعه ای از MAC Address ها را در یک Pool تعریف کرد و هربار برای هریک از VM ها، یکی از آنها را بطور dynamic و یا static (ثابت)، اختصاص داد.

نکات:

- هر بخش، 8 بیت دارد.
- 24 بیت اول، OU ID (Organizational Unit) نام دارد که مشخصه ی Microsoft بوده و ثابت است. (00155D)

برای مشاهده ی این Pool، وارد Virtual Switch manager شده و به گزینه ی MAC Address Range می رویم.
این Pool، می تواند حداکثر 256 آدرس داشته باشد. به همین جهت آخرین بخش آنها، 00 و FF خواهد بود. که به معنای 0 تا 255 است.

برای تنظیم V-MAC، وارد VM Setting شده و در زیرگزینه های Network Adapter، وارد Advanced Features می شویم.
اگر بر روی dynamic باشد، به شکل خودکار از آن Pool آدرس دریافت می کند.
اگر بر روی Static باشد، می توان آن را به دلخواه تغییر داد.

:(Quality of Service) Hyper-V QoS

وقتی چندین VM روی یک Host وجود دارند، بطور طبیعی چندین Virtual Disk هم روی Disk فیزیکی مربوط به Host پیاده سازی شده اند.

VM ها همگی بصورت همزمان در حال اجرا هستند و به Disk های مجازیِ روی همان Disk فیزیکی دسترسی دارند.

این امر به مرور زمان، باعث کند شدن فرآیندهای I/O روی دیسکهای مجازی می شود.

برای جلوگیری از وقوع این کُندی، می توان برای هر V-Disk اقدام به پیکربندی QOS کرد.

QOS شروع به کنترل V-Disk می کند.

این کنترل شامل مشخص کردن حداقل و حداکثر میزان I/O بر حسب ثانیه (IOpS) در آن دیسک می باشد.(I/O Operation Per Second)

QOS همچنین منابع شبکه را با تعیین اولویت‌ها برای نوع خاصی از داده‌ها، تنظیم و کنترل می‌کند.

قابلیت QOS برای دیسک های مجازی بصورت پیشفرض فعال نیست.

- ❖ برای اعمال QOS باید وارد Settings مربوط به VM شده و در بخش Hardware وارد SCSI Controller شده و گزینه ی Hard Drive را Expand کرده و گزینه ی Quality of Service را انتخاب کرد.
- ❖ گزینه ی Enable Quality of Service Management را فعال می کنیم.
- ❖ در نوارهای Minimum و Maximum به ترتیب مقادیر حداقل و حداکثر عملیات IOPS را مشخص کرد.

برای دریافت یک پیش زمینه از سطح ورود و خروج داده ها یا I/O در ثانیه، می توان از Resource Metering استفاده کرد.

این فعال سازی را از طریق PowerShell نیز می توانیم انجام دهیم.(مثلاً برای ماشین مجازی VM1)

```
Set-VMHardDiskDrive -VMName VM1 -ControllerType SCSI -ControllerNumber 0 -MinimumIOPS 10 -MaximumIOPS 500
```

: SR-IOV و VMQ

فرض کنید که بر روی یک سیستم (Host) و درون کنسول HyperV ، چند VM داریم.

برای اینکه هریک از Client های شبکه، به این VM ها دسترسی داشته باشند، این سیستم Host است که تعیین می کند ترافیک شبکه، به چه شکل به آنها هدایت شود.

VMQ قابلیتی است که توسط HPF (Hardware Packet Filtering) یک اولویت بندی و محدودیت برای VM ها در استفاده از CPU درنظر می گیرد تا به این شکل، خود CPU سیستم Host کمتر درگیر کنترل نیازهای VM ها شود.

با فعال سازیِ آن، VM بطور مستقیم با External NIC، یعنی NIC فیزیکی روی سیستم Host، مرتبط می شود.پس دیگر نیازی به این نیست که داده های آنها، ابتدا توسط سیستم عامل ماشین Host به سیستم عامل ماشین Guest یا همان VM کپی شوند!

پس سرعت و کارایی بهبود می یابند.

برای فعال سازی قابلیت VMQ (Virtual Machine Queues)، باید وارد Setting مربوط به VM شده و در قسمت Network Adapter گزینه ی Hardware Acceleration را انتخاب کرده و و در کادر سمت راست، گزینه ی Enable VM Queue را فعال می کنیم.

و یا در PowerShell:

```
Enable-NetAdapterVmq -Name "Ethernet *"
```

❖ از VMQ فقط زمانی می توان استفاده کرد که شبکه ی فیزیکی که NIC فیزیکی به آن متصل است، دارای سرعت 10Gbps و یا بیشتر باشد و قابلیت VMQ را نیز پشتیبانی کند. اگر سرعت آن، کمتر باشد، VMQ بصورت خودکار غیرفعال می شود.

در همین تب، می توانیم گزینه ی Enable SR-IOV را نیز فعال کنیم.

این گزینه دقیقاً کار درگاه های PCIe فیزیکی انجام می دهد به این شکل که فقط یک مسیر را جهت انتقال داده ها اختصاص می دهد.
البته باید همزمان این قابلیت را برای VSwitch هم فعال کنیم.
توسط این قابلیت، چند VM می توانند از NIC فیزیکی که روی یک درگاه PCI Express روی ماشین Host قرار دارد، بصورت اشتراکی استفاده کنند که باز هم باعث افزایش سرعت و کارآیی می شود.
گاهی نیاز هست که این قابلیت، در تنظیمات BIOS یا UEFI کامپیوتر Host، فعال شود.

برای اینکه استعلام بگیریم که قابلیت SR-IOV برای یک VM فعال است یا خیر، وارد آن شده و درج می کنیم:

```
Get-NetAdapterSriov -Name "Ethernet *"
```

: Virtual NAT

می دانیم که وقتی یک **Switch** از نوع **Internal** باشد، دارای یک **IP Range** دلخواه است که به صورت دستی، میان **Client** ها تنظیم شده است.

حال فرض کنید بخواهیم تعدادی **VM** ایجاد کنیم که تحت یک شبکه ی **LAN** با یکدیگر در ارتباط باشند. اما با دنیای بیرون هم ارتباط داشته باشند، فقط به طور ناشناس.

- در حقیقت این روش فقط در مورد **VM** های **HyperV** کاربرد دارد.
- آنها را توسط یک **V-Switch** از نوع **Internal** با هم شبکه می کنیم. (مثلاً در محدوده ی **10.10.0.0** آدرس دهی می کنیم)
- آدرس **DNS Server** شبکه ی اصلی فیزیکی را به عنوان **DNS Address** آنها وارد می کنیم.

- سیستم **Host** باید مثل **Default Gateway** برای **VM** ها عمل کند، پس آدرس **IP** آداپتوری که برای **Internal V-Switch**، در سیستم **Host** ایجاد شده است را در رنج **VM** ها تنظیم می کنیم. (مثلاً **10.10.0.1**) و یا توسط **PowerShell**:

```
New-NetIPAddress 10.10.0.1 -PrefixLength 24 -InterfaceAlias "vEthernet (InternSW)"
```

نکته: در حقیقت، با توجه به اینکه درون **Host**، یک **NIC Adapter** از شبکه ی مجازی **Internal** هم موجود است، پس از درون **Host** به سادگی می توان به **VM** ها **Ping** کرد.

اما از درون **VM** ها، نمی توان به **Host** و شبکه ی خارجی ای که **Host** به آن متصل است، **Ping** کرد.

پس اگر بتوانیم یک خط اتصال میان **Adapter** مجازیِ **Internal** که درون **Host** ایجاد شده است، با **Adapter** ای که به شبکه ی فیزیکی متصل است، برقرار کنیم، **VM** ها هم می توانند **Host** را **Ping** کنند و هم به اینترنت وصل شوند.

- با یک نام دلخواه، یک اتصال **NAT** برای این شبکه ی مجازی، درون سیستم **Host** تنظیم می کنیم:

```
New-NetNat -Name VNet -InternalIPInterfaceAddressPrefix 10.10.0.0/24
```

: Hyper-V User Deligation

فرض کنید بخواهیم یک User را فقط برای مدیریت و کنترل HyperV قرار دهیم.
که بتواند در سیستم خودش که یک Windows Server بوده و عضو Domain نیست، اما به صورت فیزیکی یا VPN، به شبکه متصل است، کنسول HyperV را کنترل کند.

1. در AD، یک User معمولی با عضویت Domain Users، برای آن کاربر ایجاد می کنیم.
2. در سیستم متعلق به آن کاربر، یک Windows Server نصب کرده و آنرا عضو Domain می کنیم. (Member Server می شود)
3. درون این Member Server وارد Computer Management و قسمت Local Users and Groups و پوشه ی Groups می شویم.
4. User ایجاد شده را به عضویت دو گروه Hyper-V Administrators و Remote Management در می آوریم.
5. حال فقط سرویس Hyper-V را بر روی آن نصب می کنیم و خارج می شویم.
6. به آن کاربر، مشخصات User ایجاد شده را می دهیم.
7. حال اگر کاربر با این User وارد این Member Server شود، تنها می تواند HyperV و VM ها را کنترل کند.

:(Direct Device Assignment) DDA

فرض کنید نیاز باشد و قصد داشته باشیم یک قطعه ی سخت افزاری که توسط درگاه PCI به سیستم متصل می شوند را بطورمستقیم به یک VM اختصاص دهیم.

- ابتدا قطعه را در Mainboard دستگاه، نصب و متصل می کنیم.
- درایور آن را در دستگاه Host نصب می کنیم.
- آن را در Host، غیرفعال یا Disable می کنیم:

```
Dismount-VMHostAssignableDevice
```

- آن را به VM متصل یا assign و سپس Mount می کنیم:

```
Add-VMAssignableDevice
Mount-VMHostAssignableDevice
```

نکته: البته برای مشاهده ی دستورات کامل در این زمینه، می توان از دستور زیر استفاده کرد:

```
Get-Command *device* -Module Hyper-V
```

: Linux VM

1.ابتدا یک VM ایجاد می کنیم:

```
New-VM -Name vm4 -MemoryStartupBytes 2GB -Generation 2 -Path F:\VMs
```

از آنجایی که Block Size های Virtual Disk های HyperV، بطور default برابر با 32mb هستند، نصب یک سیستم عامل Linux بر روی آنها، فضای زیادی را بیهوده اشغال می کند.

2.یک VHD با Block Size پایین، ایجاد می کنیم.

```
New-VHD -Path ‘F:\VMs\VM1.vhdx’ -SizeBytes 20GB -Dynamic -BlockSizeBytes 1mb
```

3.Vdisk را به VM متصل می کنیم:

```
Add-VMHardDiskDrive -VMName vm4 -Path f:\VMs\Lnx.vhdx
```

4.اگر نسخه ی Linux، نسخه ی سطح بالایی نباشد، باید Secure Boot را غیرفعال کرد، وگرنه که Micrsft UEFI Certificate :

```
Set-VMFirmware -VMName vm4 -EnableSecureBoot Off
```

: Linux Improvement

در جهت اجرای بهتر و سرعت بالاتر این سیستم ها، نیاز به نصب دو بسته ی زیر در Linux VM ها خواهیم داشت:

- **LIS** (Linux Integration Services)
- **BIS** (FreeBSD Integration Services)

اما باید دقت داشت که در برخی نسخه های Linux، مثل Ubuntu و Cent OS از قبل این بسته ها وجود دارند.

برای بررسی آن، اگر در سیستم Linux وارد Terminal شده و دستور lsmod را وارد کنیم، از میان نتایج، باید دو گزینه ی hv-netvsc و hv-storvsc وجود داشته باشند که نشانه ی وجود این دو بسته می باشند.

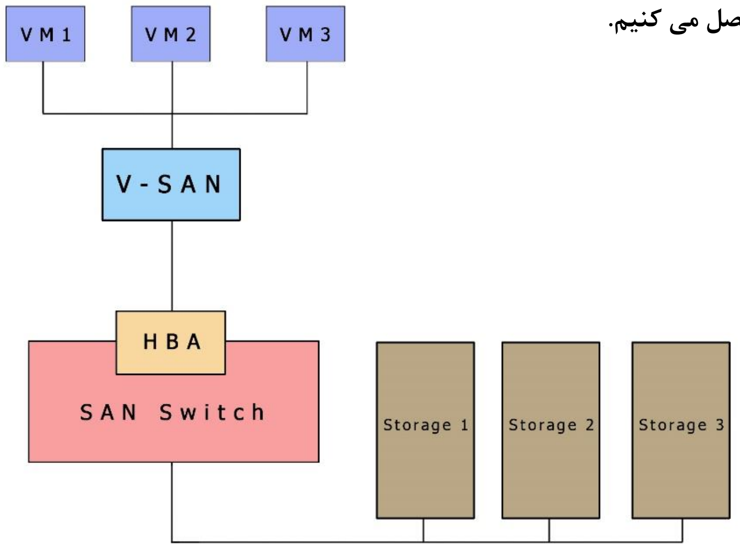
در غیراینصورت، باید آنها را از سایت Microsoft دانلود کرده و نصب کنیم.

1. در گوگل درج می کنیم: microsoft LIS و وارد لینک بالاترین ورژن برای Download Linux Integration Services می شویم.
2. وارد دکمه ی Download شده و گزینه های فایل PDF و آخرین ورژن lis-rpms را با فرمت tar.gz دانلود می کنیم.
3. از طریق راهنمای درون فایل PDF، آن را نصب می کنیم.

: Virtual SAN

برای اینکه بتوان از SAN Switch ها برای HyperV هم استفاده کرد، باید قابلیت NPIV (N Port ID Virtualization) را پشتیبانی کنند. و از طرف دیگر، در سیستم Host، درگاه HBA هم باید قابلیت NPIV را پشتیبانی کند؛ که سپس در صورت فعال نبودن، باید آن را فعال کرد.

حال در HyperV باید یک Virtual SAN را از نوع Fiber Channel (FC) ایجاد کرد.
VM ها را توسط این VSAN به SAN Switch و Storage ها متصل می کنیم.



برای راه اندازی یک Virtual SAN:

- در کادر سمت راست HyperV، وارد Virtual SAN Manager می شویم.
- بر روی Create کلیک می کنیم.
- حال اگر درگاه HBA به سیستم Host متصل باشد، یک لیست از پورتهای FC نمایش داده می شود که می توان انتخاب کرد و این VSAN را ایجاد کرد.

برای VM ها به Virtual SAN:

- وارد Setting هریک از VM ها شده و در Add Hardware گزینه ی Fiber Channel Adapter را انتخاب و Add می کنیم و سپس برای Virtual SAN، گزینه ی VSAN ای که ایجاد کردیم را انتخاب کرده و OK و تمام!

RDMA و RSS (Receive Side Scaling) :

همانطور که می دانیم حجم اطلاعات داده ای که در شبکه انتقال داده می شوند، به سرعت افزایش می یابند.
پردازش و مدیریت این نقل و انتقالات داده ای در شبکه از وظایف اصلی CPU های سیستم های عضو شبکه است.
این افزایش حجم داده ها، قدرت بیشتری از CPU را به خود اختصاص می دهد و در نتیجه قدرت کمتری از CPU ها برای پردازش کارهای دیگر در دسترس خواهد بود.
پس از کارت شبکه هایی استفاده می کنیم که فناوری RoCE (RDMA over Converged Ethernet) یا «RDMA بر روی درگاه شبکه ی متقارن» را پشتیبانی می کنند.

RDMA (Remote Direct Memory Access) دسترسی مستقیمِ حافظه ی یک Host را به حافظه ی Host دیگر بدون دخالت CPU و سیستم عامل فراهم می کند که باعث تقویت سرعت انتقال و اجرای Host با کاهش latency (تأخیر)، کاهش بار CPU و افزایش Bandwidth می شود.
RDMA با پشتیبانی از آداپتور شبکه برای انتقال داده ها به طور مستقیم به حافظه و یا از حافظه ی نرم افزار، از طریق شبکه، نیاز به کپی داده ها در Buffer سیستم عامل را از بین می برد.
چنین انتقالاتی هیچ نیازی به اینکه توسط CPU انجام شوند، ندارند و همینطور نیازی به حافظه های ذخیره شده (Cache) یا سوئیچ های Context را ندارد و انتقال ها به موازات سایر عملیات سیستم ادامه می یابد.
پس هنگامی که یک برنامه درخواست خواندن یا نوشتن را توسط RDMA انجام می دهد، داده های برنامه به طور مستقیم به شبکه تحویل داده می شوند.
در حقیقت انتقالات بر روی NIC انجام می شوند.

مزایای RDMA :

- **High Throughput** (بازدهی بیشتر)
- **Low Latency** (تاخیر کمتر)
- **High Messaging Rate**
- **Low CPU Utilization** (بکارگیری کمتر CPU)
- **Low Memory Bus Contention** (تداخل Bus Memory کمتر)
- **Message Boundaries Preserved**
- **Asynchronous Operation** (پشتیبانی از عملیات غیرهمزمان)

زمانی که سیستم Host، از شبکه DATA دریافت می کند، آنها را جهت پردازش، در اختیار CPU قرار می دهد.
محدودیت ورودی/خروجی در شبکه، باعث ایجاد نوعی Bottleneck (کاهش کاذب توان عملیاتی) از لحاظ سرعت، درCPU می شود.
RSS به توان شبکه ای Host کمک می کند و این کار را توسط توزیع کردن ترافیک I/O بین چندین CPU بجای فقط یک CPU و یا بین چند هسته از CPU بجای فقط یک هسته از آن، انجام دهد.
پس توسط RSS، از حداکثر توان CPU یا CPU ها استفاده خواهد شد.
برای استفاده قابلیت RSS، باید NIC کامپیوتر و Driver آن، حتما قابلیت RSS را پشتیبانی کنند.
در حال حاضر اکثر NIC ها و نیز vNIC ها از RSS پشتیبانی می کنند.
در بسیاری از سیستم عامل های Server، قابلیت RSS بصورت پیشفرض روی NIC و vNIC ها فعال می شود.
RSS مربوط به vNIC ها را با vRSS نشان می دهند.
همواره باید مطمئن شد که این قابلیت فعال است و در صورت فعال نبودن، باید بتوان آنرا فعال و پیکربندی کرد.

پس برای این منظور:

- در سیستم **Host**، وارد کنسول **Device Manager** شده و روی **NIC** مورد نظر راست کلیک کرده و گزینه **Properties** را انتخاب می کنیم.
- در تب **Advanced** و در لیست **Property**،گزینه ی **Receive Side Scaling** را انتخاب کرده و در کادر **Value** گزینه ی **Enabled** را انتخاب می کنیم.
- حال **RSS** فعال شده است، اما می توان گزینه های زیر را نیز تغییر داد:

- **Max Number of RSS Processors** : مشخص کردن حداکثر تعداد **CPU** هایی که توسط **RSS** مورد استفاده قرار گیرند.
- **Maximum Number of RSS Queues** : تعداد صف های **Job** های پردازشی **RSS** باید مساوی یا بزرگتر از تعداد **CPU** های قابل استفاده توسط **RSS** باشد.

- **RSS** را می توان با دستور زیر در **PowerShell** فعال و پیکربندی کرد:

```
Enable-NetAdapterRSS -Name "Ethernet0"
```

- برای اینکه در **PowerShell** استعلام بگیریم که قابلیت **RSS** فعال است یا خیر:

```
Get-NetAdapterRss
```

البته در تنظیمات تب **Advanced** مربوط به **VM**ها، گزینه ای به نام **Remote Direct Memory Access (RDMA)** هم وجود دارد که با فعال سازی آن، سیستم فیزیکی، دسترسی مستقیم به حافظه ی **VM** را بدهد. یعنی بدون مشغول کردن **CPU**، بسته های **Data** بطور مستقیم عبور کنند.

برای اینکه در **PowerShell** استعلام بگیریم که این قابلیت فعال است یا خیر و سپس آنرا فعال کنیم:

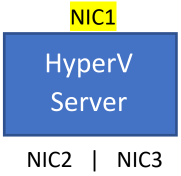
```
Get-NetAdapterRdma
Enable-NetAdapterRdma "نام آداپتور"
```

نکته:

اگر بخواهیم قابلیت RDMA را برای آداپتوری که یک Team از چند NIC است (چه فیزیکی،چه مجازی) فعال کنیم، باید همه ی آن Switch های فیزیکی:

- از یک نوع و مدل و دارای **Firmware** یکسان باشند.
- قابلیت **VMQ** را پشتیبانی کنند.

Virtual NIC Teaming :



این قابلیت Bandwidth را بسیار افزایش می دهد.

فرض کنید سیستم مقابل یک DC که دارای سه NIC متصل و روشن است.
NIC1 به مودم اینترنت متصل است و NIC2 و NIC3 به شبکه ی داخلی متصل می شوند.
حال می خواهیم تمام پهنای باند دریافتی ممکن توسط این NIC ها را در HyperV برای VM ها استفاده کنیم.

- ❖ هم این NIC های فیزیکی متصل به Host و هم Virtual Machine ای که قصد اتصالش را داریم، باید قابلیت RDMA را پشتیبانی کنند.
- ❖ در پایان، NIC هایی که تیم شده اند، برای سیستم Host و یا برای VM ها، تنها یک NIC دیده می شوند.

روش اول:
Teaming توسط سیستم Host انجام می شود. (Windows Server 2016)

- ابتدا NIC های فیزیکی را در Server Manager به یک تیم تبدیل می کنیم.
- در HyperV یک Virtual external Switch ایجاد می کنیم و آن را به سوییچ Team شده، متصل می کنیم:
Microsoft Network Adapter Multiplexer Driver

- می توان آن را در V-Switch Manager و یا توسط دستور زیر، مشاهده کرد:

```
Get-VMSwitch
```

وارد هریک از VM های موردنظر شده و یک NIC ایجاد کرده و آنرا به Switch ایجاد شده، متصل می کنیم و در تنظیمات این NIC، وارد Advanced Featured شده و گزینه ی NIC Teaming را فعال می کنیم.

روش دوم: SET (Switch Embeded Teaming)
Teaming توسط یک V-Switch در HyperV انجام می شود.
درون HyperV بطور همزمان یک Switch ایجاد و NIC های موردنظر را درون آن یک Team می کنیم.
پس فقط کافی ست که دقت کنیم که هیچ NIC Teaming ای در Server Manager انجام نشده باشد، و سپس درون PowerShell درج می کنیم:

```
New-VMSwitch -Name sw1 -NetAdapterName "Ethernet0","Ethernet1","Ethernet2" -EnableEmbeddedTeaming $true
```

وارد هریک از VM های موردنظر شده و یک NIC ایجاد کرده و آنرا به Switch ایجاد شده، متصل می کنیم و در تنظیمات این NIC، وارد Advanced Featured شده و گزینه ی NIC Teaming را فعال می کنیم.

- ❖ توسط این روش، حداکثر تعداد NIC هایی که می توان برای Teaming استفاده کرد، 8 عدد می باشد.
- ❖ NIC های فیزیکی متصل به Host که توسط این روش روی آنها NIC Teaming انجام می دهیم، نباید به یک Switch فیزیکی یکسان متصل باشند؛ بلکه هریک، به یک Switch متفاوت.

برای بررسی اینکه آیا این Teaming اعمال شده است یا خیر، از دستور زیر استفاده می شود:

```
Get-VMSwitch
```

نکته: همچنین می توان قابلیت RDMA را بر روی سوییچ مجازی Team شده نیز فعال کرد.

: VM relocation

برای جابجایی و انتقال VM ها از یک HyperV Server یا Host به یک HyperV Server دیگر، سه روش وجود دارد:

: Import / Export a VM

برای Export کافی ست بر روی VM، کلیک راست کرده و Export را زده و یک آدرس را برای ذخیره ی آن انتخاب کنیم.

```
Export-VM -Name vm1 -Path f:\
```

پس از چند دقیقه، خواهید دید که پوشه ای به نام آن VM ایجاد شده که شامل سه پوشه ی زیر می باشد:

Snapshots : اگر Snapshot ای از آن VM گرفته باشیم.

V Hard Disks : فایل حافظه ی مجازی آن

Virtual Machines : تنظیمات آن VM

برای Import کردن یک VM، کافی ست بر روی آبجکت Server در کادر سمت چپ کنسول HyperV، کلیک راست کرده و Import Virtual Machine را بزنیم.

- خود پوشه ی اصلیِ VM ای که export گرفتیم را انتخاب می کنیم.
  - **Register the virtual machine in-Place** : ماشین مجازی را از همان پوشه ای که هست، راه اندازی می کند.
  - **Restore the virtual machine** : ماشین مجازی را به مکانی کاملاً مشابه با آدرسی که قبل از Export قرار داشته، می برد.
  - **Copy the Virtual Machine** : برای کپی کردن یک VM بکار می رود.

البته برای Import کردن در PowerShell باید، فایل موجود در پوشه ی Virtual Machines با پسوند vmcx. را انتخاب کنیم:

```
Import-VM -Path "F:\vm4\Virtual Machines\255B14AB-DBE8-46F3-8B3D-BDDF20CFA1EB.vmcx"
```

: HyperV Storage Replica

- ✓ جهت ایجاد یک نسخه Replication از Virtual Machine موجود روی یک host به روی یک Host دیگر کاربرد دارد.
- ✓ هردو Host مبدا و مقصد باید در یک Domain باشند.
- ✓ اگر Host ها در Site ها یا در Domain های مختلف باشند، باید یک Trust Relationship بین آنها برقرار باشد.
- ✓ هردو از یک Firewall استفاده کنند.
- ✓ هیچیک عضو هیچ Cluster ای نباشند.
- ✓ عملیات Hyper-V Replica یک عملیات Asynchronous است.
- ✓ فرآیند Failover در آن بصورت خودکار فعال نیست.
- ✓ هیچ احتیاجی به ویژگی های پیشرفته ی شبکه مثل shared Storages و Failover Cluster ندارد.

به سیستمی که دارای VM بوده و باید از آنها یک نسخه ی Replicate ثبت شود، Primary Server گفته می شود.
به سیستمی که عملیات Storage Replica را برای VM های Primary Server انجام می دهد، Replica Server گفته می شود.

عملیات Hyper-V Replica وابستگی زیادی به قابلیت Checkpoint دارد.
در حقیقت تغییرات VM در سیستم Primary Server تبدیل به Checkpoint شده و به Replica Server منتقل می شوند.
پس Replica Server با استفاده از Checkpoint های دریافتی از Primary Server اقدام به load کردن VM می کند.

Hyper-V Replica به دو صورت قابل پیاده سازی است:

روش یک طرفه:

- **یک Host نقش Primary و دیگری نقش Replica را بر عهده دارد.**
- **در این حالت انتقال Checkpoint ها فقط از Primary به Replica انجام می شود.**

در این روش، فرض کنید Primary Server دچار مشکل شود و VM روی Replica Server روشن شود.
تا به اینجا مشکلی وجود ندارد.
پس از مدتی، خود Replica Server دچار مشکل می شود. حال اگر VM روی Primary Server را روشن کنیم، این VM به روز نیست،
چون Checkpoint ها از Replica Server به Primary Server منتقل نمی شوند.

روش دو طرفه:

- **هر دو Server بصورت همزمان هم Primary و هم Replica هستند.**
- **فایلهای Checkpoint در دو جهت منتقل می شوند و VM روی هر دو Host همواره بروز است.**

نکته: برای شروع عملیات، ابتدا یک نسخه ی کامل از VM به Replica Server کپی خواهد شد، که به این نسخه ی اولیه، Initial Replication گفته می شود؛ و سپس در بازه های زمانی مشخص، بین این کپی و نسخه ی اصلی، Replication انجام خواهد شد.

نکته: اینکه نوع Disk مربوط به VM از نوع Full یا Differenced باشد، مهم نیست. چون در صورت Differenced، دیسک اصلی هم به Replica Server منتقل خواهد شد.

فرض کنید در شبکه مان، دو HyperV Host راه اندازی کرده باشیم.

- در Host1 چند VM وجود داشته و فعال هستند: Primary Server.
- در Host2 هیچ VM ای وجود ندارد: Replica Server.

می خواهیم سرویس Storage Replica را به صورت دوطرفه، بین این دو HyperV Server، فعال و راه اندازی کنیم.

ابتدا باید تمام Virtual Switch هایی که در Primary Server وجود دارد را در Replica Server بطورکاملاً مشابه ایجاد کنیم.

- HyperV را تنظیم می کنیم.
  - وارد Replica Server یا Host2 می شویم.
  - وارد HyperV Setting شده و در تب Replication Configuration گزینه ی Enable... را فعال می کنیم.
  - همانطور که می بینیم، برای تبادل داده ها، دو حالت برای Authentication وجود دارد که در اینجا HTTP را انتخاب می کنیم.
    - در HTTP ، داده ها رمزنگاری نمی شوند.
    - HTTPS، داده ها را رمزنگاری می کند و یک پیشنیاز دارد:

    راه اندازی یک CA Server در سرور Active Directory و ایجاد یک Self-signed Certificate که در همین گزینه ی Rep. Configuration ، با دکمه ی Select Certification، این Self-signed Certificate را انتخاب می کنیم.
  - در پایین همین تب، دو گزینه وجود دارند که در اینجا گزینه ی ..Allow replication from any را می زنیم.
    - بر طبق این گزینه، هر HyperV Server عضو شبکه، به عنوان Primary Server در نظر گرفته می شود.
    - توسط Browse یک مسیر را برای فایل های Replicate شونده، در این Host تعیین می کنیم.
  - اگر گزینه ی دوم را بزنیم، روی Add کلیک می کنیم تا تعیین کنیم که کدام Server در شبکه، Primary Server باشد.
    - برای specify primary Server، آدرس FQDN مربوط به Primary Server را درج و در گزینه ی پایین آن، یک مسیر را برای فایل های Replicate شونده ی این HyperV Host تعیین می کنیم و در نوار پایین، باید نام یک گروه از Host های قابل اعتماد را درج کنیم، که اگر ابتدای نام Domain را درج کنیم، خودش پیشنهاد می دهد که چه درج کنیم.

نکته: باید دقت کنیم که پورتی که در قسمت Authentication درج شده بود را (معمولاً 80 یا 443) باید در Firewall همه ی VM ها و در Firewall خود Host ها آزاد بگذاریم.

- وارد WF.msc شده و در Inbound Rules گزینه ی Hyper-V Replica HTTP Listener (TCP-In) را برای HTTP یا HTTPS پیدا و کلیک راست کرده و enable را می زنیم.
- برای تنظیم این گزینه در Firewall مربوط به Client ها (VM ها)، وارد Active Directory شبکه شده و ابتدا آبجکت های Computer همه ی VM ها را درون یک OU قرار می دهیم؛ سپس در Group Policy Management یک GPO ایجاد کرده و آن را به OU مربوط به VM ها اختصاص داده و آن را تنظیم می کنیم. به مسیر زیر می رویم:

Computer Configuration > Policies > Windows Setting > Security Settings >
Windows Firewall with Advanced Sec.. > Windows Firewall.. >

- حال بر روی Inbound Rules کلیک راست کرده و New Rule را می زنیم.
- Port را انتخاب کرده و برای specific local Ports، عدد 80 را درج کرده و سپس Allow the Connection را انتخاب کرده و یک نام درج کرده و تمام.
  - همه ی این تنظیمات را بطورکاملاً مشابه، در Host1 نیز انجام می دهیم.

- VM ها را تنظیم می کنیم.
  - بر روی هریک از VM ها کلیک راست کرده و Enable Replication را می زنیم.
  - برای Replica Server، سرور Replica را درج می کنیم.
  - گزینه ی ...Compress the Data that is را فعال نگه می داریم.
  - اگر بیش از یک Disk در VM باشد، می توانیم تعیین کنیم که کدام یک Replicate شود و کدام نشود.

- سپس می توانیم تعیین کنیم که هرچندوقت یکبار، Replicate انجام شود، در اینجا 5 دقیقه را می زنیم.
- در تب Config. Additional Rec. Points، گزینه ی Create Additional hourly.. را زده و اگر VM موردنظر، دارای اطلاعاتی است که به سرعت در حال تغییر و به روزرسانی می باشند (مثل SQL Server و Exchange Server) گزینه ی VSS را نیز فعال می کنیم.
- در تب Initial Replication Method:
  - تعیین می کنیم که Initial Replication به چه شکل منتقل شود که اگر VM دارای حجم عظیمی از اطلاعات باشد، (چندین Giga Bytes) پس گزینه ی using external media را می زنیم که ابتدا در مکانی درون این Primary Server ذخیره شود و سپس آنرا به Replica Server منتقل کنیم، در غیراینصورت، گزینه ی over the network را می زنیم؛ و گزینه ی آخر هم در صورتی انتخاب می شود که از قبل یک کپی از این VM بر روی Replica Server موجود بوده باشد، و حال فقط یک Restore از این VM را به آن ارسال می کند.
  - در بخش Schedule Initial Replication، تعیین می کنیم که Initial Replication چه زمانی انجام شود؛ یا فوراً، و یا در تاریخ و ساعت خاصی.

برای مشاهده ی تنظیمات هریک از VMها، ابتدا آن را انتخاب کرده و در کادر پایین HyperV، تب Replication را باز می کنیم.

تنظیمات HyperV Replica :

پس از پایان ایجاد یک Initial Replication، اگر بر روی VM موردنظر کلیک راست کنیم، توسط گزینه ی Replication می توان این Replica را کنترل کرد.

- برای قطع کامل این عملیات، گزینه ی Remove Replication را می زنیم.

- برای روشن کردن و بازیابی VM موجود در Replica Server همراه با آخرین تغییرات VM موردنظر، بر روی آن کلیک راست کرده و از گزینه های Replication، گزینه ی Failover را می زنیم.
  - اگر بخواهیم عملیات Failover را تست و بررسی کنیم، Test Failover را می زنیم، و پس از آن، برای قطع این Test، دوباره کلیک راست کرده و اینبار Stop Test Failover را می زنیم.

- اگر VM موردنظر در Primary Server، دچار مشکل شود، باید نسخه ی موجود در Replica Server را تبدیل به نسخه ی اصلی کنیم و نسخه ی موجود در Primary را به نسخه ی فرعی تبدیل کنیم و عملیات Replication را انجام دهیم که نسخه ی خراب شده، دوباره بازیابی شود. پس بر روی نسخه ی Primary Server کلیک راست کرده و از گزینه های Replication، گزینه ی Planned Failover را زده و در پنجره ی باز شده، گزینه ی .Reverse the repli را فعال کرده و Fail Over را می زنیم.

- برای تغییر کامل جهت Replication، یعنی تعویض جای Replica Server با Primary Server، کافی ست ابتدا گزینه ی Failover را برای VM در Replica Server، فعال کنیم.
سپس دوباره روی آن کلیک راست کرده و از گزینه های Replication، گزینه ی Reverse Replication را بزنیم و این Wizard را تا انتها پیش ببریم، فقط برای آدرس Replica Server باید آدرس Host1 را درج کنیم.

- در حقیقت می توان نسخه ی موجود در Replica Server از یک VM را در یک HyperV Server سوم هم، replicate کرد.
برای اینکار بر روی VM موردنظر در Replica Server کلیک راست کرده و از گزینه های Replication، گزینه ی Extend Replication را می زنیم و Wizard ظاهر شده را بطورمشابه پیش می بریم.
اگر این گزینه وجود ندارد، به دلیل برقرار بودن حالت Failover است که باید ابتدا آن را قطع کرد.

: Live Migration

- ✓ گزینه ای مناسب برای زمانی است که VM روشن است و نباید خاموش شود.
- ✓ خود Virtual Machine را انتقال می دهد.
- ✓ بر روی VM هایی که نوع Disk آنها از نوع Differenced باشد، قابل انجام نیست.
- ✓ HyperV Server های مبدا و مقصد باید دارای مشخصات و تنظیمات یکسان باشند.
- ✓ رابطه ی HyperV Server ها را برای انتقال VM ها، توسط یک Network مجزا و فقط مخصوص Migration تعیین می کنیم. پس درصورت نیاز، یک NIC دیگر باید در HyperV Server ها نصب و راه اندازی کنیم و آنها را عضو یک شبکه ی جداگانه برای اینکار کنیم.
- ✓ معمولاً برای انجام این قابلیت، QOS را نیز فعال می کنند.

انواع Migration ها:

- ❖ **Live Migration (LM):**
  - در این حالت، فقط خود Virtual Machine با تمام تنظیماتی که دارد، منتقل می شود؛ و Disk آن منتقل نمی شود.
  - پس باید تمامی V-Disk ها در یک Shared Storage تحت شبکه قرار داشته باشند.
  - سرعت بالایی دارد.
- ❖ **Shared Nothing Live Migration (SNLM):**
  - هیچ Shared Storage ای در شبکه وجود ندارد.
  - باید Virtual Machine ها را بطور کامل همراه با Disk هایشان منتقل می شوند.
  - سرعت کمتری دارد.
- ❖ **Storage Migration (SM):**
  - در این حالت، فقط خود Virtual Disk مربوط به VM منتقل می شود و خود VM منتقل نمی شود.

نکته: در هرسه ی این حالات، VM های موردنظر می توانند روشن باشند، بدون هیچگونه خللی در کار آنها!

نکته: در عملیات Live Migration، ورژن و نوع Windows Server ها مهم نیستند، بلکه نوع و مدل CPU های مبدا و مقصد مهم هستند.

Deploy SNLM :

1. **HyperV Server را تنظیم می کنیم.**

وارد HyperV Setting شده و در قسمت Live Migrations :

- گزینه ی ...Enable incoming and را فعال می کنیم.
- در زیر آن می توانیم با درج یک عدد، تعیین کنیم که تا چه تعداد VM اجازه ی مهاجرت همزمان را داشته باشند.
- با انتخاب ...use any available net، از شبکه ی NIC متصل و برقرار، جهت مهاجرت استفاده می کند.
- با انتخاب ...use these IP، باید Add را زده و آدرس شبکه ی تنظیم بر روی NIC مجزا برای مهاجرت را درج کنیم و OK.

در زیرگزینه های خود گزینه ی Live migrations در سمت چپ، وارد Advanced Features می شویم:

در Authentication Protocol :

- اگر CredSSP (default Authentication Protocol of HyperV) را بزنیم، باید Host2 (مقصد) درحالت Log On باشد که به مانع Authentication برخورد نکند.
- اگر Use Kerberos را بزنیم، نیازی به Log On بودن مقصد نیست.

در Performance Options نوع انتقال اطلاعات را مشخص می کند:

- TCP/IP : پایین ترین سرعت را دارد و بیشترین استفاده از CPU را داشته و پهنای باند بالایی نیاز دارد.
- Compression : اطلاعات را فشرده کرده و سپس ارسال می کند. سرعت بهتری نسبت به حالت قبل دارد.
- SMB : باید گزینه های SMB و RDMA را فعال کرده باشیم. بالاترین سرعت را دارد.

دقیقا همین تنظیمات را برای Host2 نیز انجام می دهیم.

2. **پیشنیاز مربوط به Kerberos را انجام می دهیم.**

- وارد Active Directory شده و وارد تنظیمات آبجکت کامپیوتر HyperV Server 1 می شویم.
- وارد تب Delegation شده و گزینه ی Trust this Computer for delegation to specified Services Only را و سپس Use Kerberos Only (اگر جواب نداد، گزینه ی ...Use any) را انتخاب کرده و روی Add کلیک می کنیم.
- روی Users or Computers کلیک کرده و کامپیوتر HyperV Server 2 را Add می کنیم و در پنجره ی باز شده (Add Services) به طورهمزمان سرویس های cifs (سرویس مربوط به SMB) و Microsoft Virtual System Migration Service را انتخاب و OK می کنیم و تمام!

دقیقا همین تنظیمات را برای آبجکت HyperV Server 2 نیز انجام می دهیم.

بجای اینکه این عملیات را تک تک بر روی Host ها انجام دهیم، می توان یک Group ایجاد کرده و بر روی آن انجام دهیم و Host ها را به عضویت این Group در بیاوریم.

3. **SNLM را برای VM1 در Host1 به Host2 انجام می دهیم.**

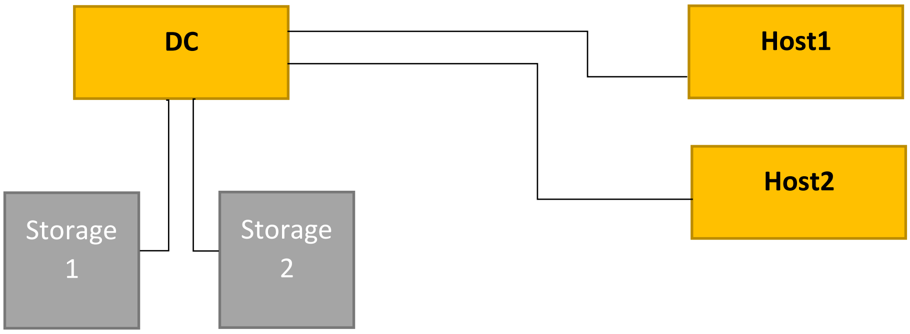
- برای اطمینان از صحت عملیات، می توان VM1 را روشن کرد.
- بر روی VM1 کلیک راست کرده و Move را می زنیم.
- می توانیم تعیین کنیم که VM همراه با Storage اش منتقل شود (SNLM) و یا فقط Storage آن که حالت SM خواهد بود.
- برای Destination Computer، آدرس Host2 را وارد می کنیم.
- در تب Choose Move Options:
  - فقط یک مکان را در مقصد، برای همه ی Disk ها و فایل های مرتبط با VM ها در مقصد، در نظر می گیرد.
  - برای هریک از VM ها، می توانیم برای هریک از Disk های VMها، یک مکان در مقصد را تعیین کنیم.
  - حالت سوم، LM می باشد.
- اگر حالت دوم را انتخاب کنیم؛ در تب Advanced Options for the Move:
  - تمام محتویات و فایل های مرتبط با VM را با هم منتقل می کند.
  - برای Virtual Disk مربوط به VM، می توانیم تعیین کنیم که کجا منتقل شود.
  - می توانیم تک تک فایل های مرتبط با VM را تعیین کنیم که کجا منتقل شوند.
- یک مکان در HyperV Host2 تعیین می کنیم و تمام!

:Deploy SM

همانطور که گفته شد، برای انجام یک LM، نیاز به یک Shared Storage در شبکه می باشد.
پس باید Vdisk مربوط به VM موردنظر، بر روی Shared Storage باشد.
پس ابتدا باید یک Shared Storage راه اندازی کنیم تا سپس Vdisk ها را به آن منتقل کنیم.

1. یک Shared Storage ایجاد می کنیم.

- در سیستم DC، وارد Server Manager شده و در تب File and Storage Services، در قسمت Shares و توسط دکمه ی Tasks، گزینه ی New Share را می زنیم.
- گزینه ی SMB Share – Application را انتخاب می کنیم.
- در تب بعد، یک مسیر را در جایی درون حافظه ی متصل به سیستم یا شبکه، تعیین می کنیم.
- یک نام برای آن درج کرده (مثلاً SharedSTG) و به مسیر تعیین شده برای آن در شبکه دقت می کنیم.
- نیازی به تنظیمات encryption نیست.
- بر روی Customize Permissions کلیک کرده و در تب Permissions دکمه ی Add را زده و توسط Select a Principal ، کامپیوترهای HyperV Server 1 و HyperV Server 2 را اضافه کرده و Type هریک را Allow انتخاب و Permission Type را بر روی Full Control تنظیم می کنیم و تمام؛ و در پایان Create را می زنیم. (و یا می توان یک Group ایجاد کرده و بر روی آن انجام دهیم و Host ها را به عضویت این Group در بیاوریم. که در اینصورت باید این گروه را برای Share Permission مربوط به Shared Storage هم اضافه کرد.)



2. به HyperV Server ها Delegation استفاده از Shared Storage ایجاد شده را می دهیم.

- برای اینکه سیستم ها بتوانند با یک Shared Storage به سادگی و بدون دردسرهای Login/out با Server ای که آنها را کنترل می کند، تبادلات داشته باشند، باید به آنها Delegation مربوط به آن Server را اعطا کرده باشیم.
- پس وارد AD شده و وارد Properties مربوط به آبجکت HyperV Server 1 می شویم.
- وارد تب Delegation شده و گزینه ی Trust this Computer for delegation to specified Services Only را و سپس Use Kerberos Only (اگر جواب نداد، گزینه ی ...Use any) را انتخاب کرده و روی Add کلیک می کنیم.
- روی Users or Computers کلیک کرده و سرور DC را Add می کنیم و در پنجره ی باز شده (Add Services)، سرویس cifs (سرویس مربوط به SMB) را انتخاب و OK می کنیم.

دقیقا همین تنظیمات را برای آبجکت HyperV Server 2 نیز انجام می دهیم.

3. Storage Migration را انجام می دهیم.

نکته: در حقیقت در این حالت هم VM می تواند روشن باشد، بدون اینکه در این روند، خللی برای آن ایجاد شود.

- بر روی VM1 کلیک راست کرده و Move را می زنیم.
- Move the virtual machine's Storage را می زنیم.
- سپس move to a single location را زده و برای location for VM، آن مسیر Shared Storage در شبکه را درج می کنیم.

راه اندازی LM :

در این روش، باید از قبل، **Virtual Disk** مربوط به **VM** موردنظر، بر روی **Shared Storage** قرار داشته باشد.

1. **Live Migration** را برای یک **VM** از **Host1** به **Host2** انجام می دهیم.
   - بر روی **VM1** کلیک راست کرده و **Move** را می زنیم.
   - **Move the virtual machine** را می زنیم.
   - برای **Destination Computer** آدرس **Host2** را وارد می کنیم.
   - گزینه ی **Move only the Virtual Machine** را انتخاب می کنیم و تمام!

OS Level Virtualisation :

ما می توانیم بدون ایجاد کردن یک سیستم عامل جدید و مجزا، یک **Virtual System** ایجاد کنیم، که مجازی سازی در لایه ی سیستم عامل خواهد بود.
این روش، یک روش مجازی سازی **Server** است که طی آن، هسته یا **Kernel** سیستم عامل این اجازه را می دهد که چندین سیستم عامل مجازی، در درون یک سیستم عامل، بصورت کاملا ایزوله ایجاد شوند.
در واقع یک سیستم عامل اصلی وجود دارد که همه چیز بر پایه ی هسته ی همین سیستم عامل بنا نهاده شده است و سیستم عامل جدیدی که به ما داده می شود نیز بر پایه ی هسته ی همان سیستم عامل اولیه خواهد بود.

به این **instance** که مشابه با **Virtual Machine** است و توسط **OS Level Virtualisation** ایجاد می شود، **Container** یا **Virtualization Engine** و یا **VE** گفته می شود.

این سیستم مجازی **Container** که در اختیار کاربر قرار می گیرد، اینطور به نظر می رسد که در حال کار کردن با یک سیستم کاملا واقعی و مستقل است، در حالی که این سیستم، کاملا مجازی و وابسته به هسته ی سیستم عامل اصلی است.
علاوه بر مکانیزم ایزوله کردن هسته یا کرنل اصلی سیستم عامل، می توان منابع را بر اساس نیاز هر **Container** نیز مدیریت کرد.

Container ها روشی برای جاسازی یک برنامه‌ی کاربردی در یک جعبه‌ی ایزوله‌شده‌ی مختص به آن برنامه می‌باشند.
برنامه‌ی کاربردی که در **Container** قرار می گیرد، از دیگر برنامه‌ها و **Process** هایی که در خارج از جعبه‌اش قرار دارند، هیچ اطلاعی ندارد.
هر آنچه که این برنامه‌ی کاربردی برای اجرای موفقیت‌آمیز به آن احتیاج دارد، درون این **Container** قرار دارد.
این جعبه به هر مکانی که منتقل شود، برای برنامه‌ی کاربردی تفاوتی ندارد و همواره به‌خوبی اجرا خواهد شد، چرا که همراه با تمام چیزهایی که برای اجراشدن نیاز دارد، درون **Container** قرار دارد.

Container ای که بر روی سیستم‌عامل اجرا می‌شود، یک **File System** دارد و می‌توان از طریق شبکه، مثل یک سیستم فیزیکی یا مجازی به آن دسترسی داشت.
نرم افزار یا ابزاری وجود دارد که وظیفه اش، ایجاد و اجرای **container** هاست به نام **Docker Engine** .
Docker، ابزاری **Open Source** است که ساخت و اجرای برنامه ها با استفاده از **Container** ها را مقدور و ساده می کند.

Docker ها همان کاری را بر روی سیستم عامل انجام می دهند که **Virtual Machine** ها بر روی سخت افزارها انجام می دهند.
Docker، سیستم عامل را بین **Application** های مختلف به اشتراک می گذارد.

- بطورکل، **Docker** ها را می توان در انواع مجازی سازی و **Cloud Platform** ها نیز استفاده کرد.

به همین جهت، یکی از معایب **OS Level Virtualisation** این است که اگر **OS** سیستم دچار مشکل شود، همه ی **Container** ها نیز متأثر می شوند.

Container به برنامه نویس این اجازه را می دهد که **Application** خود را با تمامی اجزای مورد نیاز آن، اعم از فایل های **dll** و کلیه ی **Library** ها و کلیه ی وابستگی ها، در قالب یک بسته ی نرم افزاری بیرون دهد، طوری که از بیرون، یک نرم افزار واحد به نظر برسد.
با استفاده از این مکانیزم، برنامه نویس می تواند مطمئن باشد که نرم افزاری که نوشته است، فارق از نوع سیستم عاملی که بر روی آن اجرا می شود، نیازی به نصب کردن هیچگونه اجزای جانبی برای اجرا شدن نخواهد داشت و حتی تنظیمات آن نیز بصورت از پیش تعریف شده انجام می شود.

پس مهم نیست **Docker** ها را در چه سیستمی اجرا می کنید، آن ها می توانند در هر محیطی اجرا شوند، چون وابسته به محیط نیستند.

:Container

همانطور که می دانیم، هر VM یک کپی کامل از سیستم عامل را دارد، که شامل دردسرهای زیر می باشند:

- هریک از VM ها نیاز به نصب و راه اندازی یک سیستم عامل کامل دارد، که قدرت پردازش بالایی را می طلبد.
- برای این سیستم عامل ها باید License فراهم شود که هزینه ای جداگانه خواهد داشت.
- این Server ها باید رسیدگی و نگهداری شوند.
- تحرکت و جابجایی VM ها ساده نیست.

به همین دلایل، لزوم استفاده از Container ها پدید آمد.

به این شکل که از Container ها و Virtual Machine ها بطور همزمان و با هم استفاده می کنیم.

پس Container ها، App ها و Service ها را ایزوله و ارائه می کنند، و نه یک ویندوز کامل را!!

مزایای Windows Container ها:

- fast
- Isolation
- Portability
- Density (جمع و جور و در کنار هم)

به دو شکل می توان Container تحت Microsoft را ایجاد کرد:

- Windows Container :

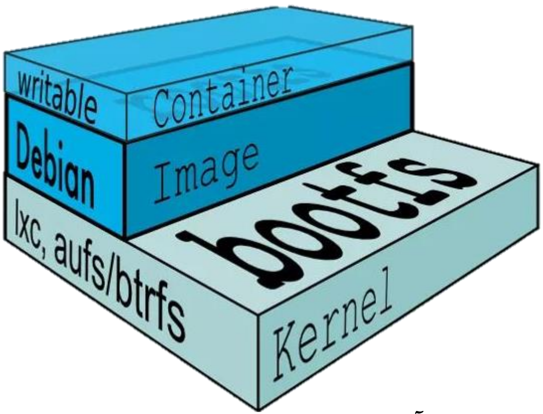
بر روی Kernel سیستم عامل Windows اقدام به ایجاد Container می شود.

به این صورت که ابتدا Base OS را نصب و راه اندازی می کنیم و سپس Docker را نصب می کنیم و توسط آن، Container ها را.

- HyperV Container :

همانطور که می دانیم، برای راه اندازی Container ها، نیاز به ابزار Docker می باشد.

- Docker مبتنی بر LXC (Linux Containers) می باشد.
- اجرای Docker، در هر سیستمی که می‌تواند Docker را اجرا کند، امکانپذیر است، مثل: Linux، MAC، Windows و ... .
- پس از نصب و راه اندازی Docker در ویندوز، برای ایجاد Container، نیاز به یک Image خواهیم داشت.
- یک docker image شامل محیط و Package های مورد نیاز برای اجرا Application ها می باشد.
- وقتی یک image را اجرا می کنیم، یک instance به عنوان Container اجرا می شود.
- در حقیقت، Container ها از قلب docker Image ها بیرون می آیند.
- بنابراین یک Container، یک instance از اجرای یک docker image می باشد.
- Docker image از کرنل Host (سیستمی که Docker روی آن نصب شده است) برای اجرا استفاده می کند.



مخزنی از Image های Docker وجود دارد، به نام Docker Hub که بیش از 14 هزار Image در آن وجود دارد.

Container Implementation :

1. Base OS را راه اندازی می کنیم.

- بر روی آن Windows Server نصب و آن را عضو Domain کرده و هیچ Service یا Role دیگری روی آن نصب نمی کنیم.
- آن را Active کرده و Firewall آن را خاموش کرده و به شکل یکپارچه در شبکه، به اینترنت متصل کرده (مثلاً NAT) و کاملاً Update و یکبار Restart می کنیم.
- Feature مربوط به Containers را نصب می کنیم:

```
Install-WindowsFeature containers -Restart
```

2. Docker را نصب می کنیم.

- برای دریافت بسته ی دستورات مربوط به مدیریت Docker، از مخزن PowerShell، دستور زیر را وارد می کنیم:

```
Install-Module -Name DockerMSftProvider -Repository PSGallery -Force -Verbose
```

نکته: اگر سوال پرسید، Yes را زده و اگر خطایی داد؛ ویندوز را Update و سپس PSgallery را نیز Update می کنیم.

- آخرین نسخه ی ابزار Docker را (به صورت Online) نصب می کنیم:

```
Install-Package Docker -ProviderName DockerMsftProvider -Force -verbose
```

- سیستم را یکبار Restart می کنیم:

```
Restart-Computer -Force
```

نکته: برای اطمینان از نصب Docker و یا مشاهده ی ورژن Docker نصب شده، درج می کنیم:

```
Get-Package -Name Docker -ProviderName DockerMsftProvider
```

نکته: برای اطمینان از Run بودن سرویس Docker ؛ و در صورت Run نبودن، Run کردن آن:

```
Get-Service docker
Start-Service Docker
```

نکته: برای استعلام Online اینکه آخرین نسخه ی موجود برای Docker کدام است، درج می کنیم:

```
Find-Package -Name Docker -ProviderName DockerMsftProvider
```

نکته: برای upgrade نسخه ی Docker موجود در سیستم، دو دستور زیر را به ترتیب درج می کنیم:

```
Install-Package -Name Docker -ProviderName DockerMsftProvider -Update -Force
Start-Service Docker
```

نکته: دستورات مربوط به docker به صورت زیر اجرا می شوند.

برای دریافت همه ی دستورات آن، از help-- استفاده می شود.

```
docker نام دستور
docker --help
```

docker version	اطلاع از ورژن Docker
	مشاهده ی docker Image های موجود برای microsoft

3. Container Image ها را نصب می کنیم.

- یکبار سیستم را Restart می کنیم.

نکته: هربار که سیستم را Restart می کنید و یا یک دستور نصب را اجرا می کنید، بهتر است دوباره سرویس docker را چک کنید که در حال اجرا باشد:

```
Start-Service Docker
```

- توسط دستور زیر، ابتدا لیست Docker Image های موجود را مشاهده می کنیم:

```
docker search microsoft
```

- برای Windows Server دو Image موجود است: NanoServer و WindowsServerCore که هر دو را در لیست می بینیم.
- حال باید این دو Image را نصب کنیم؛ اما قبل از آن، باید بسته ی دستورات Container Image را نصب کرد:

```
Install-PackageProvider ContainerImage -Force
```

- برای مشاهده ی این دو:

```
Find-ContainerImage
```

- حال باید یکی از این دو **Image** را دانلود و نصب کنیم، که هم از طریق دستورات **Docker** و هم توسط دستورات **Container** های ویندوز می توان این کار را انجام داد.

نکته: NanoServerImage دارای حجم 400MB و WindowsServerCore دارای حجم 6GB می باشد.

برای نصب Base Image هریک از آنها :

```
docker pull microsoft/windowsservercore
docker pull microsoft/nanoserver
```

و یا

```
docker pull mcr.microsoft.com/windows/servercore:1607
docker pull mcr.microsoft.com/windows/nanoserver:1803
```

برای نصب Base Image هریک از آنها در Windows Server 2019 :

```
docker pull mcr.microsoft.com/windows/servercore:ltsc2019

docker pull mcr.microsoft.com/windows/nanoserver:1809
```

- پس از دانلودِ آن، برای مشاهده ی **Image** های **Docker** موجود، دستور زیر را درج می کنیم:

```
docker images
```

:Remote Desktop Services

در حقیقت این Role، نسخه ی قدرتمند و کامل همان Remote Desktop ای است که در ویندوزهای معمولی هم وجود دارد که شامل چند ابزار مهم است:

- **Session Host** : جهت راه اندازی قابلیت Remote App بکار می رود.

یکی از توانایی های این ابزار، ارائه ی نرم افزارها و برنامه های کاربردی بصورت RemoteApp می باشد.
فرض کنید شما نمی توانید نرم افزاری مثل فتوشاپ را به دلیل حجم و توانی که می طلبد، روی همه ی Client ها نصب کنید. چون Client ها ضعیف بوده و قصد ندارید برای ارتقا آنها هزینه کنید!
پس Server قدرتمندی را تهیه کرده و به جای نصب فتوشاپ روی همه ی سیستم ها، فقط روی این Server نصب می کنید.
به این سرور، RDSH (Remote Desktop Session Host) گفته می شود.
حال از طریق RemoteApp، آیکون فتوشاپ را برای هر Client ای که می خواهید، می فرستید.
هنگامی که کلاینت ها نرم افزار را اجرا کنند، تمامی فرآیندِ اجرای آن، روی Server اتفاق می افتد، اما اینطور به نظر می رسد که نرم افزار روی سیستم خود Client نصب است.

- **Web Access** :

این ویژگی این قابلیت را ممکن می کند تا برنامه هایی که قرار است در اختیار Client ها قرار بگیرند، بصورت Web-base و توسط مرورگر استفاده شوند.
هنگامی که Web Access پیکربندی شود، کاربران می توانند با ورود به وبسایت، لیست همه ی برنامه های قابل اجرا از طریق RemoteApp را مشاهده کنند.

- **Connection Broker** :

شما با استفاده از Network Load Balancing یا اجرای DNS round robin می توانید شمار زیادی از سرورهای RDS را در یک Farm (مجموعه ای بزرگ) قرار دهید، طوری که بصورت یک Server برای کاربران تشخیص داده شوند.
RDS farm بهترین راه برای پشتیبانی از تعداد بالای کاربران است و برای افزایش عملکرد Farm، می توان از Connection Broker استفاده کرد.
RD Connection Broker به کلاینت ها کمک می کند تا به RDS Farm متصل شده و اگر ارتباطی قطع شد، آن را Reconnect کند.

- **Virtualization Host** :

فرض کنید روی RDS، یک یا چند ماشین مجازی روی Hyper-V ایجاد کرده اید.
توسط این ویژگی، می توان به این ماشین های مجازی متصل شد.
Client ها می توانند توسط این ابزار، به یک VM متصل شوند.
و یا توسط RD Connection Broker، می توان یک pool یا Farm از چندین VM ایجاد کرد و Client ها به آن متصل شوند.

- **Gateway** :

با استفاده از این ابزار، کاربرانی که احراز هویت شده اند، می توانند توسط اینترنت، به کامپیوترهای Session Host که در شبکه ی داخلی قرار دارند، متصل شوند.
به این ابزار RD Gateway گفته می شود و توسط تونل HTTPS، امنیت این ارتباط را فراهم می کند.
با ایجاد دسترسی کاربران احراز هویت شده، به کامپیوترهای شبکه داخلی، توسط یک ارتباط RD Gateway، نیاز به شبکه های خصوصی مجازی (VPN) مرتفع می شود.

VDI (Virtual Desktop Infrastructure) :

- تکنولوژی **VDI** جهت راه اندازی دسکتاپ های مجازی مورد استفاده قرار می گیرد.
- در سازمان های بزرگ که تعداد کارمندان و تعداد سیستم ها زیاد است، جهت کاهش هزینه و مدیریت متمرکز، **VDI** راه اندازی می شود.
- در **Server** ای به نام **RDVH** ، درون **Hyper-V** به تعداد سیستم های مورد نیاز، ماشین مجازی (**VM**) می سازیم.
- این **VM** ها در سرور **RDVH** فعال می شوند تا در کنار **RemoteApp** ها در صفحه ی **RDWeb** به نمایش درآیند.
- با اینکار سیستم فیزیکی کاربر، تنها نقش یک رابط را ایفا می کند تا از طریق آن بتوان به دسکتاپ های مجازی متصل شد.
- از آنجاییکه این دسکتاپ های مجازی همگی ماشین مجازی هستند، به نسبت کاربردی که قرار است داشته باشند، می توان آنها را تنظیم کرد. (مثلاً **CPU, RAM, NIC** و هارد دیسک های متفاوت به آنها **Assign** کنیم)

نکته: ارتباط میان **Client** ها با **RDS** رمزنگاری شده می باشد، پس پیشنیاز راه اندازی این **Server** یک **CA Server** می باشد.

برای راه اندازی آن، به ترتیب **Role** های زیر باید نصب شوند:

- RDWeb (Remote Desktop Web Access) :

یک رابط کاربری تحت وب است که هم نرم افزارها را و هم دسکتاپ ها را برای **Client** ها نمایش می دهد.
با نصب رول **RDweb** نقش **IIS** هم نصب و کانفیگ می شود تا صفحه ی **RDWeb** را میزبانی نماید.

- RDCB (Remote Desktop Connection Broker) :

در ساختار شبکه ی خود، ممکن است **RemoteApp** و **VDI** را در کنار هم راه اندازی کنیم، پس در این موارد وقتی کاربر وارد صفحه ی **RDweb** می شود، می تواند انتخاب کند که به یک **RemoteApp** متصل شود و یا به یک **Virtual Desktop**!
RDCB آن را به یکی از این دو سرور **RDSH** یا **RDVH** انتقال می دهد یا **Redirect** می کند.
علاوه بر این ممکن است در شبکه به جهت **High Availability** یا **Load Balancing** بیش از یک **RDVH Server** راه اندازی کرده باشیم. در این موارد **RDCB** در کانکشن های زده شده به سرور، **Balance** ایجاد می کند.

- RDSH :
- RDVH :
- RDGateway :
- RD Licensing :

سرویس های **RemoteApp** و **VDI** به صورت پیشفرض، بدون **License** تا ۴ ماه قابل استفاده می باشند.
جهت استفاده ی مداوم، باید به ازای هر کاربر، یک لایسنس خریداری شود.
سپس با راه اندازی **RD Licensing server** و وارد کردن لایسنس ها در آن، محدودیت ۴ ماهه از میان می رود.
روند کار به این صورت است که زمانی که یک کاربر به سرور **RDSH** یا **RDVH** وصل می شود و تقاضای سرویس می کند، سرور مربوطه از **RD Licensing server** استعلام می گیرد که آیا این کاربر لایسنس دارد یا خیر.

RDS Implementation :

1. کنسول Remote Desktop Services را نصب می کنیم.

- در Server Manager و Add Roles and Features وارد شده و در همان ابتدا، در تب select installation type، گزینه ی Remote Desktop Services را می زنیم.
- اگر بخواهیم این سرویس را بر روی چند Server راه اندازی کنیم، گزینه ی Standard و اگر بخواهیم تنها بر روی یک Server آن را راه اندازی کنیم، گزینه ی Quick Start را می زنیم.
- گاهی در شبکه، کاربرانی هستند که هیچگونه کیس و سیستم و سیستم عاملی نداشته و تنها یک مانیتور یا Zero client دارند که به Server متصل هستند و Server تنها یک دسکتاپ مجازی در اختیار آنها قرار می دهد، پس در اینجا گزینه ی Virtual Machine Based Desktop Deployment را انتخاب می کنیم.

اما Server در حالت Session Based Desktop Deployment تنها یک نرم افزار را در شبکه منتشر می کند و هیچ دسکتاپ مجازی ای در اختیار قرار نمی دهد. کاربرها خودشان سیستم دارند و تنها برای استفاده از نرم افزار ها، به این Server متصل می شوند.

- پس گزینه ی دوم را انتخاب کرده و نصب را تا پایان پیش می بریم و یکبار Restart می کنیم.

2. ابزارهای Remote Desktop Services را نصب می کنیم.

- در Server Manager و Add Roles and Features وارد شده و Role مربوط به Remote Desktop Services را انتخاب کرده و در تب Role Services، همه ی گزینه ها را فعال کرده و نصب و یکبار Restart می کنیم.

و یا توسط PowerShell به ترتیب دستورهای زیر را وارد می کنیم:

```
Install-WindowsFeature Remote-Desktop-Services
Install-WindowsFeature RDS-connection-broker -IncludeAllSubFeature
Install-WindowsFeature RDS-Gateway -IncludeAllSubFeature
Install-WindowsFeature RDS-Licensing -IncludeAllSubFeature
Install-WindowsFeature RDS-RD-Server -IncludeAllSubFeature
Install-WindowsFeature RDS-Virtualization -IncludeAllSubFeature
Install-WindowsFeature RDS-Web-Access -IncludeAllSubFeature
```

- در Server Manager از بخش Tools وارد Remote Desktop Licensing Manager می شویم.
- در کادر سمت چپ، بر روی آبجکت Server کلیک راست کرده و Properties را می زنیم.

Remote Desktop Licensing :

می دانیم که در حالت معمول، توسط Remote Desktop Connection فقط دو نفر (دو session) می توانند بطور همزمان به سرور remote شوند.

اما پس از نصب نقش Remote Desktop Services، تعداد این افراد بی شمار خواهد بود.

البته این قابلیت مربوط به این سرویس، از هنگام نصب سرویس، فقط تا 90 روز رایگان خواهد بود؛ سپس باید License آن را خریداری کرده و فعال کنیم.

به همین منظور، باید سرویس Remote Desktop Licensing را نیز نصب و پیکربندی کنیم.

برای نصب آن نیز از طریق Server Manager پیش رفته و Role مربوط به Remote Desktop Services را نصب می کنیم.

Map :

افزونه ی Microsoft Assessment and Planning Toolkit بعد از آنالیز کردن سیستم، گزارش کاملی را ارائه داده و کمک خواهد کرد که راه درستی را جهت Update سیستم انتخاب کنیم.
این ابزار هم برای ویندوزهای Client و هم و برای استفاده های Server ها و مجازی سازی، Database و Cloud نیز قابل استفاده است.

به این صورت که اطلاعات موردنیازش را توسط ارسال Query به همه ی اعضای شبکه، جمع آوری و درون یک SQL Database ذخیره می کند.

برای دریافت این نرم افزار در گوگل سرچ می کنیم : map Microsoft
وارد لینک جدیدترین Download Microsoft Assessment and Planning Toolkit شده و دکمه ی Download را می زنیم.
گزینه ی MapSetup.exe را انتخاب و دانلود کرده و نصب می کنیم.

برای دسترسی به آن در Start وارد Microsoft Assessment and Planning Toolkit می شویم.
یک Name برای پایگاه داده ی آن درج کرده و OK.
در سمت راست، سناریوهای قابل پیاده سازی را می بینیم.
اما قبل از راه اندازی هریک از آنها، نیاز به یک فهرست یا Inventory خواهیم داشت.
پس در میانه ی صفحه، وارد Perform an inventory می شویم.

- در تب اول، باید تعیین کنیم که چه سیستم هایی از شبکه، Scan شوند.
- در تب Discovery Methods تعیین می کنیم که به چه روش هایی، اعضای شبکه را پیدا کند.
- در تب AD Credentials نام main DC و مشخصات یک حساب Admin را وارد می کنیم.
- در تب AD Options تعیین می کنیم که تمام OU ها و Container ها بررسی شوند، یا بخش خاصی فقط!
- در تب Scan IP Range محدوده ی IP که قصد داریم بررسی شود را تعریف می کنیم.
- در تب All Computers Credentials باید Account هایی را جهت بررسی Client های شبکه مشخص کنیم.

  پس Create را زده و یکبار فقط WMI را فعال کرده و مشخصات یک حساب را (معمولاً Admin شبکه) برای اتصالهای ویندوزی تحت شبکه، وارد کرده و SaveAndNew را می زنیم.

  و برای بقیه ی موارد هم به همین شکل، اما با User های متفاوت، انجام می دهیم.
- و بقیه ی تب ها را می توانیم بدون تغییر تا پایان پیش ببریم.

باید احتمالاً چند دقیقه ای صبر کنیم تا این Scan به پایان برسد و Close بزنیم.
در پایان می بینیم که یک تعداد ماشین را Found یا پیدا کرده است و با یک تعداد ارتباط برقرار کرده است (Inventoried).

حال اگر در کادر سمت چپ، وارد گزینه ی Environment شویم، می بینیم که چه تعداد ویندوز Server و غیر Server و یا Linux را پیدا کرده است. و می توان بر روی هریک از بخش کلیک کرد و با جزییات بیشتر مشاهده کرد.

برای بررسی توانایی های موجود جهت Virtualization یا Cloud می توان بر روی گزینه ی هریک کلیک کرده و تنظیمات موردنیاز را انجام داد و دوباره Scan کرد.

:Active Directory Federation Service

همانطور که می دانیم برای برقراری ارتباط بین دو شبکه ی Forest یا Domain کاملاً متفاوت، از Trust استفاده می کنیم که از طریق سرویس LDAP انجام می گیرد.

اما برقراری Trust هم معایبی دارد:

- اگر تعداد Trust ها زیاد شوند، مدیریت آنها، کار بسیار دشواری می شود که روی عملکرد و طراحی امنیت شبکه تاثیر خواهد داشت.
- Firewall مجبور خواهد بود تعداد زیادی از پورت ها را باز کند، که این کار هیچ گاه راه حل مناسبی نیست.

پس از AD FS استفاده می کنیم.

توسط AD FS، کاربرهای شبکه ی A قادر به login کردن در شبکه ی B خواهند بود، بدون اینکه هیچ Account ای در شبکه ی B داشته باشند.

قابلیت AD FS سه قابلیت را پشتیبانی کرده و انجام می دهد:

❖ Identity Federation :

- می دانیم که وظیفه ی AD DS انجام Authentication در شبکه است. و این Authentication را تنها در محدوده ی شبکه ی خودش برای Client هایی که به Domain خودش متصل باشند، انجام می دهد.
- حال فرض کنید در یک شبکه ی دیگر [شبکه ی B] ، نرم افزاری وجود دارد که یکی یا برخی از کاربران شبکه ی ما قصد استفاده از آن را دارند.
- روش اول این است که برای همه ی آن کاربرهای موردنظر، یک Account هم در شبکه ی B ایجاد کنیم و Credential آن حساب ها را به Client ها ارسال کنیم.
- روش دوم به این شکل است که ابتدا باید AD FS را بر روی شبکه ی خودمان راه اندازی کنیم، تا تحت قابلیت Identity Federation، ابتدا یک trust بین آن Software و شبکه ی ما برقرار شده و سپس کاربران ما به سادگی به شبکه ی B متصل شده و در آن، توسط حسابی که در شبکه ی خودمان دارند، Login کنند، تا به سادگی آن نرم افزار را باز کنند.
  - ✓ به نرم افزاری که در شبکه ی B، تحت AD FS به شبکه ی ما trust کرده است، Relay Party گفته می شود.
  - ✓ به AD FS شبکه ی ما، Identity Provider گفته می شود.

❖ Claim-based Authentication :

- درحقیقت وقتی یک Client از شبکه ی A درخواست دسترسی به نرم افزار در شبکه ی B را ارسال می کند، آن نرم افزار جهت بررسی این درخواست، آن را به AD FS در خود شبکه ی A می فرستد تا وضعیت آن را جویا شود.
- AD FS برای بررسی آن درخواستی که از شبکه ی خودش به شبکه ی B ارسال شده است، با AD DS خودش پرس و جو انجام می دهد.
- در پایان، AD FS پاسخی را به آن Software در شبکه ی B ارسال می کند، که شامل حق دسترسی و سطوح دسترسی آن کاربر می باشد.
- به این فرآیند، Claim-based Authentication گفته می شود.

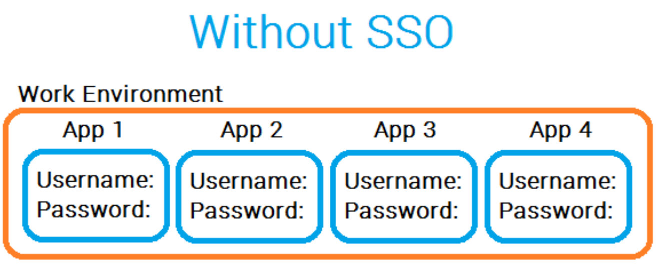
❖ Single sign on (SSO) :

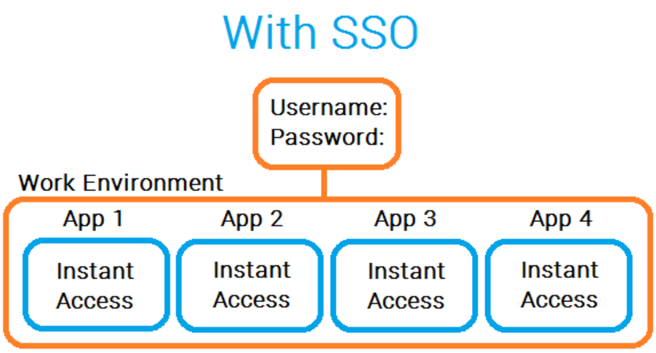
- این قابلیت، این مزیت را فراهم می کند که وقتی یک Client یکبار به Software شبکه ی B متصل شد و login کرد، دیگر در دفعات بعدی، نیازی به وارد کردن دوباره ی credential اش جهت login نخواهد بود.
- استفاده از SSO مزایای بسیار زیادی همانند کاهش هزینه، افزایش بهره بری و صرفه جویی در وقت را دارد.
- کاربران تنها لازم است یک کلمه عبور را به یاد داشته باشند و احتمال فراموش کردن کلمه عبور کاهش می یابد. ضمن آنکه تنها یک بار کلمه عبور از کاربر سوال خواهد شد.

ویژگی های AD Federation Services :

- AD FS کارکردی مشابه با روابط Trust دارد اما نه با استفاده از LDAP بلکه با استفاده از HTTPS و پورت 443.
- AD FS هم بر روی ویندوزهای Standard و هم Data Center قابل راه اندازی است.
- AD FS وابسته به AD CS است، تا در پیاده سازی آن برای هر Server، یک Certificate صادر کند.
- AD FS با گسترش AD RMS (Active Directory Rights Management Services) دارای مدیریت ساده تر شده است.
- Port های موردنیاز برای AD FS که باز بودن آنها آنچنان خطرناک نخواهد بود:
  - پورت 53 : برای DNS که اغلب تنها جهت استفاده ی read-only مجوز دارد.
  - پورت 80 : برای HTTP که به علت امنیت پایین، آن هم تنها جهت استفاده ی Read-Only مجوز دارد.
  - پورت 443 : برای HTTPS بکار می رود.
  - پورت 25 : برای SMTP بکار می رود.

  به صورت ایده آل تمام پورت های دیگر باید بسته باشند.
- پس از ایجاد روابط مورد نیاز میان دو Forest ، نیازی به مدیریت مستقیم این رابطه نیست، چرا که هر Forest، از سرویس ها و App های Forest دیگر استفاده کرده و روابطش و کاربرانش را خودش مدیریت می کند.





- مزیت این روش این است که هر سازمان همکار (Partner) تنها لازم است که اطلاعات احراز هویت در شبکه ی داخلی خودش را مدیریت کند، AD FS بقیه ی کار ها را انجام می دهد.
- به طور خلاصه، زمانی که نیاز به Partnership با یک سازمان دیگر باشد، AD FS پیاده سازی می شود.
- با استفاده از AD FS نیازی به استفاده از AD LDS برای Primeter Network نیست و تنها عملیات مدیریتی روی یک دایرکتوری انجام می شود.
- برای روابط B2B - Business to Business ، استفاده از AD FS می تواند بهترین راه حل باشد.

برخی محدودیت های AD FS :

- عدم دسترسی به Share Files و Print Servers
- عدم دسترسی به منابع Active Directory
- عدم دسترسی به سرور به شکل Remote

دو Role Service مهم در AD FS:

- **Federation Service: که از یک Trust Policy استفاده می کند. با استفاده از آن، در خواست های Authentication جهت صدور Token هدایت می شوند.**
- **Federation Service Proxy: یک proxy server است برای Federation Service.**

برای راه اندازی یک Federation Trust:

- **در هر دو طرف رابطه، AD FS را نصب می کنیم.**
- **میان Federation Service های هر دو طرف، یک Trust ایجاد می کنیم.**

فرض کنید Forest A قصد داشته باشد از منابعی در Forest B استفاده کند.
به Forest A گفته می شود : Account Partner
به Forest B گفته می شود : Resource Partner

AD FS Implementation :

نکته: برای راه اندازی AD FS چون راه اندازی و ارتباط میان Federation Service ها نیاز به Certification دارد، ابتدا اقدام به ایجاد Certificate برای آنها می کنیم.

1. **AD CS را راه اندازی کرده و Certificate ایجاد می کنیم.**
- بر روی **Certificate Templates** راست کلیک کرده و **Manage** را می زنیم.
- **Certificate** ای به نام **Web Server** را پیدا و **Duplicate** می کنیم.
- یک نام برایش تعیین می کنیم، مثلاً: **SSL for FS**
- در تب **Request Handling** گزینه ی **Allow Private Key to be Exported** را فعال می کنیم.
- حال باید تعیین کنیم که enroll کردن این **Certificate** بین **DC** ها و **Computer DC** ها مجاز است، پس به تب **Security** رفته و دو گروه **Domain Computers** و **Domain Controllers** را **Add** و دسترسی های **Enroll** و **Autoenroll** را فعال کرده و **OK**!
- در پنجره ی اصلی کنسول **Certificate Authority**، روی **Certificate Template** کلیک راست کرده و **Certificate to Issue** را زده و **Certificate** ای که ایجاد کردیم را انتخاب می کنیم : **SSL for FS**

2. **Certificate را نصب می کنیم.**
- وارد کنسول **MMC** شده و در Add/Remove Features و کادر سمت چپ، گزینه ی **Certificates** را **Add** می کنیم.
- Computer Account را انتخاب کرده و تا پایان پیش می رویم و هردو پنجره را **ok** کرده و در صفحه ی اصلی MMC، در سمت چپ و زیر مجموعه ی Certificates، روی Personal کلیک راست کرده و All Tasks و Request new Certificate را می زنیم.
- در تب **Request Certificate**، روی لینک آبی رنگ زیر **Certificate** ای که ایجاد کردیم (**SSL for FS**) کلیک می کنیم.
- **Type** مربوط به **Subject name** را بر روی **Common name** قرار داده و برای **Value** باید یک نام همراه با نام **Root Domain** درج کنیم، مثلاً:

Fs.payamavar.local

- آن را **Add** می کنیم.
- **Type** مربوط به **Alternative name** را روی **DNS** قرار داده و **Value** آن را نیز مثل بالا درج کرده و **Add** و **OK**!
- تیک گزینه ی این **Certificate** را فعال کرده و **Enroll** و تمام!

3. **از این Certificate یکبار Export می گیریم.**
- پس در **Personal** و سپس **Certificates** آن را **Open** کرده و در تب **Details** گزینه ی **Copy to files** را می زنیم.
- گزینه ی **Yes, Export the Private Key** را فعال می کنیم.
- گزینه ی **.Personal Information Ex** را انتخاب و گزینه های **..Export all extended**.و **.Enable certificate p** را فعال می کنیم.
- گزینه ی **Password** را فعال کرده و یک **Password** برای آن درج می کنیم.
- یک مسیر و یک نام برای فایل **Export** تعیین می کنیم.

4. **حال اقدام به نصب Role مربوط به AD FS می کنیم.**
- با فشردن گزینه ی .. **Configure** وارد تنظیمات آن می شویم.
- فعلاً .. **Create the first federation Server** را انتخاب می کنیم.
- برای **SSL Certificate** از طریق **Import** همان فایل **Certificate** که **Export** گرفتیم را انتخاب کرده و پسورد را می زنیم.
- یک نام برای این **Federation Server** تعیین می کنیم.
- برای **Account Name** هم می توان یک **User** معمولی و هم می توان یک **MSA** انتخاب کرد که **MSA** بهتر می باشد.
- فعلاً گزینه ی .. **Create a database on this Server using** را زده و **next** و تمام!
- وقتی که نصب تمام شد، باید سیستم را یکبار **Restart** کنیم.
- برای تنظیمات، در **Server Manager** وارد گزینه ی **AD FS Management** می شویم.

IPAM (IP Address Management):

سرویس IP Address Management یکی از Feature هایست که از Windows Server 2012 به بعد ایجاد شد.
یک Framework مرکزی جهت مدیریت IP Address ها و سرویس های مرتبط با آن مثل DNS و DHCP می باشد.
این قابلیت یا فناوری، جهت کنترل و مدیریت پیچیدگی های شبکه هایی که دارای چند Server مختلف با آدرس دهی های متعدد هستند، کاربرد دارد.
برخی از ابزارها یا Component های IPAM به شرح زیر می باشند:

ASM (Address Space Management):

این ویژگی، مدیریت فضای شما را قادر می سازد تا یک سلسله مراتب بسیار متفاوت از فضای معمول آدرس ها در شبکه ایجاد کنیم.
از آن برای مدیریت آدرس های IPv6 و آدرس های عمومی و خصوصی IPv4 استفاده می شود.

ASM شامل یک ویژگی گزارش دقیق است که امکان ردیابی دقیق (tracking) استفاده از یک آدرس IP را دارد.

- مدیریت یکپارچه ی همه ی آدرس ها (dynamic and Static)
- تشخیص و مدیریت Conflict ها، همپوشانی و تکرار، در فضای آدرس در سراسر سیستم
- نمایش موجودی بسیار قابل تنظیم از فضای آدرسIP
- اضافه و کم کردن آدرس IP با استفاده از محیط پاورشل
- شناسایی و اختصاص آدرس های IP موجود

محدودیت های سرویس IPAM :

IPAM نمی تواند روی Domain Controller ها فعال شود، پس IPAM Server لازم است که یک Member Server باشد.
IPAM امکان Auditing را برای IPv6 فراهم نمی آورد.
یک IPAM Server تنها در یک Forest می تواند عمل کند.
IPAM تنها از Windows Server 2012 R2 به بعد امکان اتصال به SQL Server را دارد.
IPAM از سیستم های غیرمایکروسافتی جهت Configuration و Management پشتیبانی نمی کند.
اگرچه امکان Import کردن اطلاعات برای دستگاه های غیر مایکروسافتی وجود دارد.

همانطور که گفته شد، زمانی که بیش از یک Server در شبکه باشد، نیاز به IPAM Server می باشد.پس برای Implementation یا به اصطلاح Provisioning یک IPAM Server در شبکه، به دو شکل می توان عمل کرد:

- **Manual**: در این روش مجبور خواهیم بود که در ادامه ی راه اندازی، در تک تک Server ها، تمامی تنظیمات لازم را به صورت دستی انجام دهیم.

- **Group Policy based**: در این روش، کافی ست در خود IPAM Server، تمامیِ تنظیمات موردنظر را در یک فایل GPO ایجاد کرده و از طریق Powershell در خود IPAM Server، این فایل را به تمام Server های دیگر، منتقل و در آنها تنظیم کنیم و IPAM Server قادر به برقراری ارتباط با تک تک آنها خواهد بود.

وقتی یک IPAM Server برای اولین بار راه اندازی می شود:
تمامیِ DC ها و DNS Server ها و DHCP Server ها پیدا کرده و فهرست بندی کرده و در یک database ذخیره می کند.
این database می تواند یک WID (Windows Internal Database) باشد و یا یک SQL Server Database.
و بالاخره یک محیط مدیریتی جهت نظارت و کنترل بر اعضای شبکه را ارائه می دهد.

برای مدیریت Server های یک Forest دیگر در سیستم IPAM Server شبکه ی جاری، باید ویندوز مربوط به IPAM Srver کاملاً به روز و از نوع Server 2016 به بالا باشد و یک two-way Trust بین هردو Forest برقرار باشد.

IPAM Server Implementation :

ابتدا یک Windows Server 2016 روی سیستم نصب کرده و آن را عضو Domain شبکه می کنیم.

- حتماً فقط و فقط با حساب Administrator مربوط به main Domain باید وارد شویم.

در Server Manager وارد ویزارد Add Roles and Features شده و هیچ Role ای را انتخاب نمی کنیم، اما در تب Features گزینه ی IP Address Management (IPAM) را انتخاب کرده و Install می کنیم.

وارد Server Manager شده و به تب IPAM که اضافه شده است، وارد شده و تک به تک این شش مرحله را طی می کنیم:

1. البته طبق قاعده، مرحله ی اول باید انجام شده باشد و آدرس IPAM Server در زیر گزینه ی Connect to IPAM Server درج شده باشد، وگرنه که باید روی خود آن گزینه کلیک و نام سرور را انتخاب کنیم.

2. برای Provision کردن IPAM Server در شبکه، روی Provision the IPAM Server کلیک می کنیم.

- فعلاً برای Database آن، WID را انتخاب می کنیم.
- به جهت سهولت کار، Group Policy Based را انتخاب می کنیم.

نکته: هر IPAM Server ای که Group Policy Base باشد، دارای یک Prefix Name می باشد؛ پس یک پیشنام برای آن درج می کنیم.

پس از پایان نصب، می بینیم که:

- سه GPO با پیشنامی که تعیین کردیم برای DHCP Server ها و برای DNS Server ها و برای Network Policy Server ها تعریف کرده است.(هنوز ایجاد نشده اند!)
- در زیر Next Steps درج شده است که باید در PowerShell دستور Invoke را وارد کنیم تا این GPO ها ایجاد شده و به سایر Server ها، دسترسی به این GPO ها را بدهیم.
- در PowerShell دستور زیر را توسط نام Domain و پیشنامی که برای IPAM GPO تعیین کردیم، درج می کنیم:

```
Invoke-IpamGpoProvisioning -Domain payamavar.local -GpoPrefixName payamipam
```

- حال اگر به کنسول Group Policy Management برویم می بینیم که هر سه GPO ایجاد شده اند.
- حال باید تعیین کنیم که هریک از این GPO ها به کدام یک از Server ها اختصاص داده شود.
- پس هریک از GPO ها را به ترتیب انتخاب کرده و در سمت راست و تب Scope، در بخش Security Filtering دکمه ی Add را زده و Server های مورد نظر را اضافه کرده و OK!

نکته: برای تغییر GPO Prefix Name، از دستور Set-ipamConfiguration استفاده می کنیم.

برای اینکه GPO ها، به سرعت به Server ها اعمال شوند، در PowerShell توسط نام Server ها، دستور زیر را وارد می کنیم:

```
icm DC1,DC2,DC3{gpupdate /force}
```

- برای اطمینان از نتیجه ی صحیح عملیات، دستور زیر را با نام تک تک Server ها وارد می کنیم:

```
icm DC1{gpresult /r}
```

که در نتیجه، در بخش Computer Setting ونه User Setting، و زیر تیتر Applied Group Policy Objects باید نام هر سه Object درج شده باشند.

3. برای پیدا کردنِ تنظیمات Forest و وصل شدنِ IPAM به Root Domain، وارد گزینه ی Configure Server Discovery می شویم. Get Forest را زده و OK کرده و چند لحظه صبر می کنیم تا تنظیمات Forest را پیدا کند.

- دوباره وارد Confgure Server Discovery شده و اگر نام main Root و Root DC صحیح باشد، بر روی Add کلیک کرده و OK.

4. برای پیدا کردنِ Server های موجود در Domain، بر روی گزینه ی Start Server Discovery کلیک می کنیم؛

- که چند لحظه طول می کشد.

5. **برای تأیید Server ها و مدیریت دسترسی آنها، وارد گزینه ی پنجم می شویم.**

- **ستون IPAM Access Status سرورها باید unblocked باشد.**
- **بر روی هریک از Server ها راست کلیک کرده و Edit Server را زده و در Server Type نوع مدیریت آن سرور و در Manageability Status، حالت آنرا تعیین می کنیم؛ که آنرا بر روی managed قرار داده و OK!**

6. **برای جمع آوری داده های همه ی Server هایی که IPAM پیدا کرده است، در WID ای که انتخاب کردیم، بر روی گزینه ی ششم کلیک می کنیم؛ که چند لحظه طول می کشد.**

- **حال برای کار بر روی تنظیمات شبکه، می توان در همین کنسول IPAM در سمت راست هریک از گزینه ها را انتخاب کرد.**

نکته:

- برای مدیریت Server های یک Forest دیگر در سیستم IPAM Server شبکه ی جاری، باید ویندوز مربوط به IPAM Srver کاملاً به روز و از نوع Server 2016 به بالا باشد و یک two-way Trust بین هردو Forest برقرار باشد.

:DHCP and DNS Server in IPAM

مثلاً **DNS and DHCP Servers** را می زنیم.
می توانیم **DNS** ها را فیلتر کنیم که فقط آنها را ببینیم؛ پس باید از بالا **Server Type** را بر روی **DNS** قرار دهیم.

- اگر **DNS Zone** ها دریافت شده باشند، می بینیم که یا به شکل قرمز رنگ و یا سفید رنگ هستند که این به این معنی است که داده های آنها هنوز **Retrieve** یا دریافت نشده اند.
- پس روی تک تک آنها کلیک راست و **Reset** را می زنیم.
- از بالا و راست، از زیرگزینه های **Tasks**، گزینه ی **Retrieve Server Data** را زده و پس از چند لحظه، **Refresh** می کنیم!

برای ایجاد یک DNS ZONE :

- در تب **DNS and DHCP Server**، بر روی **Server** موردنظر کلیک راست کرده و **Create DNS Zone** را می زنیم.

برای ایجاد یک DNS Record :

- در تب **DNS Zones**، بر روی **Zone** موردنظر کلیک راست کرده و **Add DNS Resource Record** را می زنیم.
- در پنجره ی باز شده **New** را زده، مشخصات را وارد کرده و گزینه ی **Add Resource Record** را زده و بعد **OK** می کنیم.

DHCP Scope :

- اگر به تب **DHCP Scopes** برویم، لیست **Scope** ها را می بینیم که احتمالاً بعضی از آنها به رنگ زرد رنگ می باشند!
- طبق **IPAM Setting**، اگر تا یک میزان مشخص، از **Scope** موردنظر استفاده نشده باشد، آیکون آن زردرنگ خواهد بود که به آن **Under** گفته می شود، و اگر بیش از یک میزان مشخص، از **Scope** موردنظر استفاده شده باشد، آیکون آن قرمز رنگ خواهد بود!
- اگر میزان استفاده شده از **Scope**، بین این دو حداقل و حداکثر باشد، آیکون آن به سبز خواهد بود و به آن **Optimal** گفته می شود.

این وضعیت را می توان با انتخاب هریک از **Scope** ها، و در کادر پایین، تب **Scope Properties** و گزینه ی **Utilization** هم مشاهده کرد.

- برای تنظیم این دو میزان، می توان در بالای پنجره ی **IPAM** وارد گزینه ی **Manage** شده و سپس **IPAM Setting** و گزینه ی **Configure Utilization Threshold** را انتخاب کنیم.

:RBAC (Role based Access Control)

برای اینکه یک کاربر بتواند به Server دسترسی داشته باشد، اما فقط به بخشی از تنظیمات Server مثل یک Scope از DHCP و یا یک Zone از DNS از طریق قابلیت RBAC به صورت زیر عمل می کنیم:

- یک Role خاص را تعریف می کنیم. مثلاً:
  - Role مدیریت تمام Server ها
  - Role مدیریت فقط DHCP یا فقط یکی از Scope های DHCP
  - و ...
- یک Access Scope ایجاد کرده و آن را مثلاً به یکی از Scope های DHCP اختصاص می دهیم.
- یک Access Policy تعریف می کنیم که طبق آن یک User به Access Scope ایجاد شده، متصل می شود.
- در حقیقت به این Access Policy ایجاد شده، RBAC گفته می شود.

1. **یک Role تعریف می کنیم.**
   - در کنسول IPAM، وارد گزینه ی **Access Control** می شویم و در کادر پایین آن **Role** را انتخاب می کنیم.
   - در کادر **Role** در سمت راست و بالا، **Role** های **Default** را می بینیم.
   - در بالا از زیرمجموعه های گزینه ی **Task**، گزینه ی **Add User Role** را می زنیم.
   - یک نام درج می کنیم و در تب **Operations** یک دسترسی انتخاب کرده و **OK**!
     مثلاً DHCP Scope Operations

2. **یک Access Scope ایجاد می کنیم.**
   - در کنسول IPAM، وارد گزینه ی **Access Control** می شویم و در کادر پایین آن **Access Scopes** را انتخاب می کنیم.
   - در بالا از زیرمجموعه های گزینه ی **Task**، گزینه ی **Add Access Scope** را می زنیم.
   - دکمه ی **New** را زده، یک **Name** درج کرده و **Add** می کنیم و **OK**!

- به تب **DHCP Scopes** می رویم و همانطور که می بینیم در ستون **Access Scope** همه ی **Scope** ها، **Global** درج شده است.
- پس روی یک **Scope** موردنظر کلیک راست کرده و **Set Access Scope** را می زنیم.
- گزینه ی **..Inherit access Scope** را غیرفعال کرده و **Access Scope** ایجاد شده را انتخاب کرده و **OK**!

3. **یک Access Policy ایجاد کرده و Role ایجاد شده را به Access Scope ایجاد شده، متصل می کنیم.**
   - در کنسول IPAM، وارد گزینه ی **Access Control** می شویم و در کادر پایین آن **Access Policies** را انتخاب می کنیم.
   - در بالا از زیرمجموعه های گزینه ی **Task**، گزینه ی **Add Access Policy** را می زنیم.
   - برای **User Alias** گزینه ی **Add** را زده و **User** یا **Group** موردنظر را اضافه می کنیم.
   نکته: اگر User یا Group را پیدا نکرد، از طریق گزینه ی Locations، گزینه ی Domain موجود را انتخاب می کنیم.
   نکته: این User یا Group باید یک عضو معمولی باشد، یعنی عضو گروه Domain Users باشد و نه بیشتر.
   - در پایین روی **New** زده و در زیر آن از فهرست **Select Role**، **Role** ای ایجاد کردیم را انتخاب و **Add Setting** را می زنیم.
   - **Apply** و **OK**!

حال کافی ست یکبار با **User** ای که برای **Access Policy** اضافه کردیم، در سیستمی که **IPAM** را فعال کرده ایم، **Log in** کنیم.می بینیم که بجز تنظیمات **DHCP Scope** ای که انتخاب کردیم، هیچ تغییر دیگری نمی توانیم وارد کنیم.حتی به کنسول های **DNS** و **DHCP** هم دسترسی نخواهیم داشت!

: IP Address Spaces

در IPAM و در بخش IP Address Space، می توان IP Address ها را به شکل حرفه ای، مدیریت کرد.
می توان بطوریکجا و همزمان، تمام DHCP Server های تمام DC های شبکه را مشاهده و بررسی کرد؛ که از مزایای بزرگ آن این است که از یکسان بودن و تداخل IP Address ها درون شبکه، جلوگیری می شود.

- به این صورت که تمام آدرسهایی که با یک IP قابل آدرسدهی هستند را در یک Block قرار می دهد:

192.168.X.X

- هر Block تشکیل می شود از چندین Range :

192.168.1.X
192.168.2.X
192.168.3.X
...

- هر Range تشکیل می شود از تعدادی IP Address در یک محدوده ی منظم:

192.168.1.1
192.168.1.2
192.168.1.3
192.168.1.4
...

- یک IP Address Range می تواند یک DHCP Scope باشد.

در کنسول IPAM، و در سمت چپ، وارد گزینه ی IP Address Space و از زیرمجموعه های آن، وارد IP Address Blocks می شویم.
اگر لیست Block ها را نشان نداد، از فهرست Current View بالا، گزینه ی IP Address Blocks را انتخاب می کنیم.

ایجاد یک Block:

از گزینه ی Task بالا، Add IP Address Block را می زنیم:

- یک Network ID و یک Prefix length موردنظر درج می کنیم، مثلاً : 10.0.0.0
- اما نمی توان برای Start IP Address، مقدار Network ID را و برای آخرین آدرس، آدرس broadcast را درج کرد.
- پس آنها را تغییر می دهیم و OK!

یک Range ایجاد می کنیم:

از گزینه ی Task بالا، Add IP Address Range را می زنیم:

- یک Network ID که از زیرمجموعه های Block تعریف شده باشد، همراه با یک Prefix درج می کنیم.
- برای اینکه بطورخودکار Subnet ها ایجاد شوند، باید Automatically assign address Values را فعال کنیم.
- میزان ابتدا و انتهای Range را نیز تعیین می کنیم.
- در قسمت DNS Servers آدرس DNS Server شبکه را وارد می کنیم.
- در قسمت DNS Search Suffix، آدرس FQDN مربوط به main DC را وارد می کنیم.
- در قسمت Gateway IP Address، آدرس Gateway ای که در رنج IP Block تعریف شده باشد را وارد می کنیم.
- و Apply و OK! حال برای مشاهده ی آن، از منوی Current View، گزینه ی IP Address Ranges را می زنیم.

اگر در ستون Overlapping دقت کنید، نباید هیچ یک از Range ها دارای مقدار Yes باشد، چون به معنای تداخل آدرسها با یک Range دیگر می باشد.به جز برای Range هایی که قابلیت Failover برای آنها فعال شده است، که مشکلی ندارد!

: IP Address assignment

برای اینکه از یک Range یک IP را به یک Client اختصاص دهیم:

1. ابتدا باید آن Range را بررسی کنیم که کدامیک از آدرس های آن آزاد و کدام اختصاص داده شده اند.
   - پس روی آن Range کلیک راست کرده و Find and Allocate Available IP Address را می زنیم.
   - حال چند لحظه طول می کشد تا اولین آدرس آزاد را در جدول بالای پنجره نشان داده و آزاد بودن آن را بررسی کند، و اختصاص داده نشده باشد، مقادیر No Reply و Not Found را نشان می دهد.
2. حال یک DNS Record در آن Range تعیین می کنیم.
   - در تب Basic Configurations می توانیم MAC آدرس Client موردنظر را وارد کنیم.
   - مقدار Managed by Service را بر روی MS DHCP قرار می دهیم.
   - مقدار Service Instance را برابر با آدرس FQDN مربوط به DNS Server قرار می دهیم.
   - مقدار Assignment type را بر روی Dynamic قرار می دهیم.

   - به پایین این پنجره و قسمت DNS Record Synchronization آمده و یک Name انتخاب کرده (مثلاً PC5) و Zone و مقادیر دیگر را تعیین کرده و گزینه ی .Automatically create DNS recordsرا فعال کرده و OK!
3. آدرس اختصاص داده شده را تست می کنیم.
   - پس در خود سیستم IPAM، وارد CMD شده و درج می کنیم:

nslookup pc8

   - در پاسخ باید نام FQDN کامل و آدرس IPv4 آنرا نشان دهد.
   - اما احتمالاً آدرس IPv6 را نشان می دهد، و Name آن را نشان نمی دهد!
   - این به این دلیل است که هنوز Reverse Lookup Zone ای برای IPv6 ایجاد نشده است.
4. Reverse Lookup Zone را برای IPv6 ایجاد می کنیم.
   - به بخش DNS and DHCP Servers رفته و بر روی گزینه ی DNS Server موردنظر کلیک راست کرده و
   - Create DNS Zone را می زنیم.
   - گزینه ی IPv6 Reverse Lookup zone را و سپس Primary Zone را انتخاب کرده و برای Network ID،
   - Network ID مربوط به DNS Server را درج می کنیم؛ مثلاً: 2001:11aa:6345::
   - و Apply و OK! پس یک Reverse Lookup Zone ایجاد شد.
5. یک PTR Record برای Reverse Lookup Zone ایجاد می کنیم.
   - بر روی Zone ایجاد شده کلیک راست کرده و Add DNS resource record را می زنیم.
   - دکمه ی New را می زنیم.
   - Type را بر روی PTR قرار می دهیم.
   - در ادامه ی آدرس Host IP Address ای که درج شده، یک : و سپس مثلاً عدد 100 را درج می کنیم.
   - برای Host Name، آدرس کامپیوتر DNS Server را درج کرده و دکمه ی Add resource record را زده و OK!
   - حال اگر دوباره دستور nslookup را دوباره برای سیستم موردنظر تست کنیم، نام آن هم نشان داده می شود.

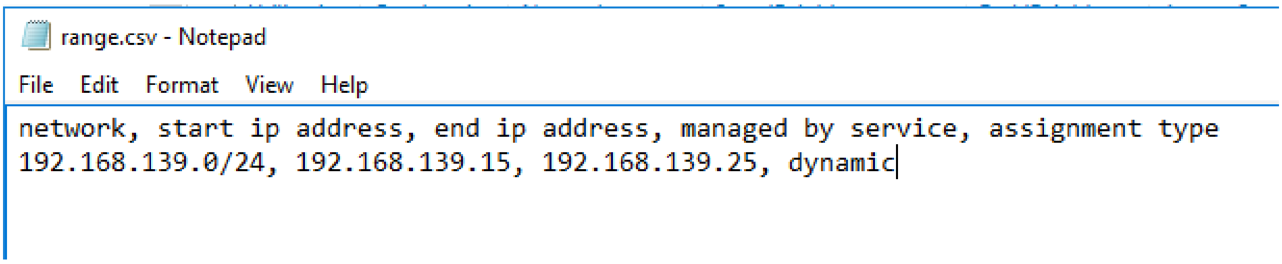
نکته: برای اینکه یک User بتواند در IPAM ببیند کدام User ها، کدام IP ها را دریافت کرده اند، باید عضو گروه IPAM IP Audit Administrators باشد.

: Importing IP infos in IPAM

فرض کنید که باید تعداد زیادی **IP Range** یا **IP Block** را وارد **IPAM** کنیم.

مثلاً ایجاد یک **IP Range** :

- ما می توانیم همه ی اطلاعات را در یک فایل **notepad** به ترتیبی که در **IPAM** در قسمت **Range** ها تعیین شده اند، درج کنیم و سپس آن فایل را در **IPAM** وارد کنیم تا اطلاعات بطور یکجا و همزمان ثبت شوند.
- یک فایل **Notepad** باز کرده و نام ستون های موردنیاز برای ثبت یک **IP Range** را به ترتیب از چپ به راست با کاما، درج می کنیم.


range.csv - Notepad
File Edit Format View Help

```
network, start ip address, end ip address, managed by service, assignment type
192.168.139.0/24, 192.168.139.15, 192.168.139.25, dynamic
```

- آن را با یک نام دلخواه و با پسوند **CSV** ذخیره می کنیم.
- در پنجره ی **IP Address Ranges** ، بر روی **Tasks** کلیک کرده و گزینه ی **Import IP Address Ranges** را می زنیم.

: Event Catalog

برای مشاهده ی تمامی تغییرات اعمال شده در کنسول **IPAM** (**Add** و **delete** و **modify** ها) می توانیم به قسمت **EVENT CATALOG** مراجعه کنیم که همیشه آخرین تغییر را در اولین سطر نشان می دهد.

همانطور که در کادر پایین سمت چپ می بینیم، می توان **Event** های **IPAM** و همچنین **Event** های **DHCP** را مشاهده کرد.

در قسمت IP Address Tracking :

- می توان به قسمت **by IP Address** وارد شد و یک **IP** مربوط به یک **Client** را و یک بازه ی زمانی را برحسب تاریخ روز، وارد کرد، تا تغییرات و رخدادهای آن را مشاهده کرد.
- می توان به قسمت **by host name** رفته و نام یک کامپیوتر را همراه با یک بازه ی زمانی وارد کرد، تا تغییرات و رخدادهای آن را مشاهده کرد.
- می توان به قسمت **by user name** رفته و یک **User name** را همراه با یک بازه ی زمانی وارد کرد، تا تغییرات و رخدادهای آن را مشاهده کرد.

برای اینکه بتوان از یک **User** عضو **Domain** برای کنترل **DHCP Server** در سیستم **IPAM Server** (به نام **Server1**) استفاده کرد، از دستور زیر استفاده می کنیم:

net localgroup "Server1\IPAM MSM Administrators" User1/add

Dynamic DNS (DDNS) :

می دانیم که آدرس IP که از ISP ها دریافت می کنیم، dynamic IP هستند که طی بازه های زمانی منظم یا نامنظم، تغییر می یابند.
فرض کنید یک Web Server یا حتی یک Game Server دارید.
در حقیقت شما هر بار که به اینترنت متصل می شوید، به دلیل عوض شدن آدرس IP دریافتی از ISP ، نام مربوط به Web Server یا Game Server که قرار است به آدرس IP تبدیل شود نیز، مرتب عوض می شود.
پس در این وضعیت، به محض تغییر آدرس IP، ارتباط Server با آن Name یا آدرسی که برای آن تعیین شده بود، از بین می رود.

در این حالت، دو راهکار وجود دارد:

- یا خریدن یک Static IP؛ که در این صورت از سمت ISP، یک IP به طور ثابت به Server داخلی شما اختصاص داده می شود.
- و یا اینکه از Dynamic DNS استفاده کنیم، که ISP ها آن را نیز ارائه می دهند.

در حالت عادی سرویس DNS یک سرویس موجود در Server است که Client ها از آن استفاده می کنند، و تنها می‌توان یک آدرس IP ثابت یا همان Static IP را برای هر Client ثبت کرد.
DDNS برای این طراحی که این محدودیت DNS را برطرف نموده و شما را قادر سازد تا بدون نیاز به IP ثابت (که تهیه ی آن هزینه ی بالا دارد) اقدام به استفاده از IP های داینامیک برای اتصال به دامنه‌های خود نمایید.

در حقیقت با به کارگیری DDNS ، نام Domain داخلی خود را به Dynamic IP های دریافت شده از ISP متصل نموده و به صورت خودکار با تغییر IP ، اطلاعات جدید، در Domain نیز بروز رسانی می شوند.
پس توسط DDNS هر بار با تغییر آدرس Server داخلی شما، اسم آن در DNS Server مربوط به ISP مطلع و به روز خواهد شد.

Dynamic DNS یک برنامه ی کوچک است که بر روی Server داخلی قرار می گیرد که در بازه های زمانی معین، آدرس IP سیستم را، به DNS Server سمت ISP ارسال می کند تا با تغییر آدرسIP ، نام Server داخلی همچنان update و در دسترس باقی بماند.

- در حقیقت مفهوم Dynamic DNS کاملاً مشابه همان dynamic Update مربوط به DNS Server داخلی در محیط Domain است.

Dynamic DNS می‌تواند برای افراد زیر مفید باشد:

- افرادی که می‌خواهند از کامپیوتر خانگی خود، به دوربین‌های مدار بسته ی تحت شبکه ای که در اداره قرار دارند، از طریق یک نام Domain دسترسی داشته باشند.
- افرادی که Application یا Website خود را میزبانی می کنند.

سایت هایی هستند که می توان با ثبت نام در آن ها، از سرویس DDNS بهره مند شد.
برخی از این سرویس دهنده ها عبارتند از:

https://www.noip.com
http://www.changeip.com
http://www.dnsexit.com
https://www.dynu.com

سبک راه اندازی سرویس دهنده های DDNS معمولا شبیه به هم است:

1. در سایت سرویس دهنده ی DDNS ثبت نام می کنید و یک Account می سازید.
2. پس از Log in در سایت، یک Host Name برای خودتان ایجاد می کنید.
3. Host name ای که ایجاد کردید را در Device مورد نظرتان استفاده می کنید، مثلا در دوربین یا مودم.
4. تنظیمات نهایی Port Forwarding را انجام می دهید.

NAT (Network Address Translation) :

NAT قابلیتی است که به Client های دارای Private IP اجازه می دهد تا از طریق Public IP که درون Router تنظیم شده است، به فضای اینترنت متصل شوند.

در واقع وقتی یک Client از قابلیت NAT بهره مند می شود، دارای هویتی دوگانه خواهد شد. یعنی به صورت همزمان با آدرس private خود در شبکه ی داخلی و با آدرس Public در اینترنت می تواند فعالیت کند.

البته تنظیمات آدرس Public، روی کارت شبکه ی Client انجام نمی شوند.

- **این پروتکل، تمام آدرس های Private که در شبکه ی داخلی هستند را به صورت Encapsulation به سمت Port خروجی که به اینترنت متصل است، ارسال می کند.**
- **در حقیقت به وسیله ی NAT می توانیم آدرس های یک شبکه را به یک شبکه ی دیگر ترجمه کنیم.**
- **NAT تقریبا در همه ی سیستم عامل ها و Router ها قابل انجام است، که هر کدام شیوه و روش خود را دارند.**

موارد مورد استفاده از پروتکل NAT :

- **جهت صرفه جویی در تعداد Public IP و هزینه**
- **جهت تغییر Public IP به دلایلی**
- **زمانی که تمام اعضای شبکه داخلی از Private IP استفاده می کنند.**
- **برقراری ارتباط بین دو شبکه که دارای رنج IP یکسانی نیستند.**

در حقیقت شرکت ها از NAT جهت Publish کردن وبسایت خود روی اینترنت استفاده می کنند و چون هکرها چیزی بیشتر از یک Punlic Address را نمی بینند، نمی توانند به Server وبسایت نفوذ کنند.

به NAT ای که از طریق ابزار RRAS راه اندازی شده باشد، Microsoft NAT Server گفته می شود.

پس برای راه اندازی RRAS، نیاز به سیستمی داریم که حداقل دارای دو NIC باشد.

اصطلاحات در زمینه ی NAT :

- **Inside Local Address : آدرس هایی که برای شبکه ی داخلی استفاده می شوند.(Private IP)**
- **Inside Global Address: آدرس هایی که دستگاه های داخلی شبکه، با آن از بیرون دیده می شوند.(Public IP)**
- **Outside Local Address: آدرسی هایی که دستگاه های داخل شبکه، دستگاه های خارج از شبکه را با آن می بینند و می تواند آدرس Private باشد.**
- **Outside Global Address : آدرس های Public مربوط به دستگاه های بیرون از شبکه، که ما با آنها ارتباط برقرار می کنیم، مانند Public IP مربوط به Server سایت IMDB.**

در حقیقت هر NAT Server درون خودش دارای یک NAT Table است که از دو ستون تشکیل شده است:

Outside Global Address	Inside Local Address

نکته: اگر بخواهیم بر روی یک Server، هم HyperV را نصب و راه اندازی کنیم و هم NAT را؛ بهتر است که ابتدا HyperV را راه اندازی کنیم و سپس NAT را، در غیراینصورت، مجبور خواهیم بود که کمی تنظیمات NAT را دستکاری کرده و یا حتی از نو انجام دهیم.

چرا که افزودن Virtual Switch در HyperV، باعث ایجاد تغییر در Adapter های Server خواهد شد!

: NAT Types

❖ Static NAT :

- در این روش هریک آدرس Private ، تبدیل به یک آدرس Public ثابت می شود یا به عبارتی یک دستگاه از شبکه ی داخلی، یک آدرسIP در شبکه ی خارجی دریافت می کند.

❖ Dynamic NAT :

- در این حالت یک مخزن یا Pool از Public IP ها وجود دارد که اگر یکی از Client ها قصد ارسال داده به اینترنت را داشته باشد، Router یک آدرس را به صورت dynamic به او اختصاص خواهد داد.
- در حقیقت شیوه ی عملکرد این NAT، مشابه با Static است، با این تفاوت که دیگر مدیرشبکه نیازی به تخصیص آدرس عمومی به خصوصی ندارد.
- تنها باید به اندازه یا بیشتر از تعداد Client ها، Public IP در Pool موجود باشد.

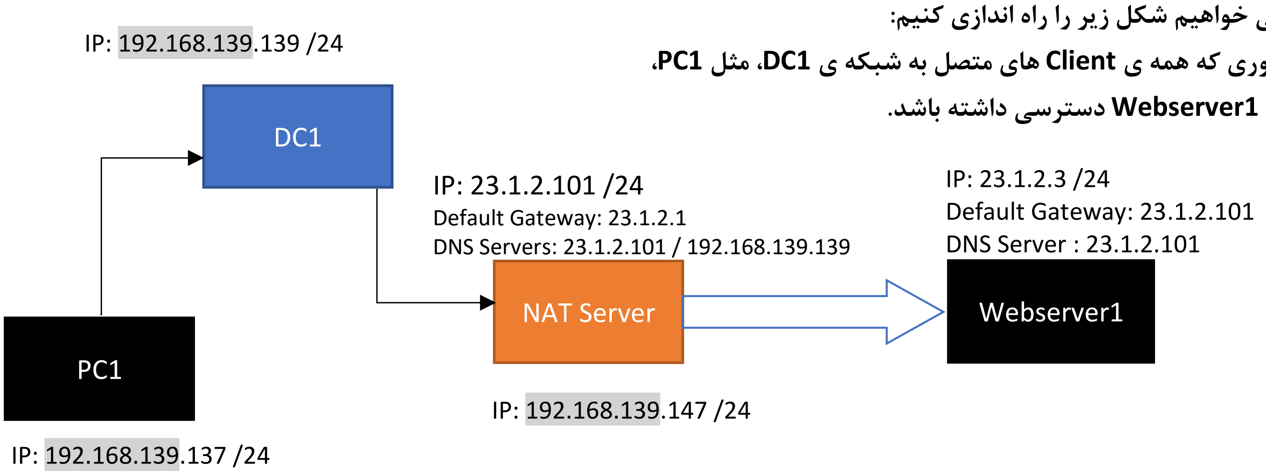
❖ Overloaded (PAT) (Port Address Translation) (Port Forwarding) :

- در این روش می توان چندین آدرس Private را با استفاده از یک Public Address به اینترنت متصل نمود.
- این شیوه از NAT بسیار محبوب و پر استفاده است.
- با استفاده از این NAT می توان تا هزاران کامپیوتر را به اینترنت متصل نمود، که باعث می شود تا استفاده از Public IP ها تا حد زیادی مدیرت شده و بهینه باشد.

Dynamic NAT(Source NAT) deployment:

- کامپیوتر **NAT Server** هم می تواند عضو **Domain** باشد و هم می تواند در حالت **Workgroup** باشد.
- تمام **Client** های شبکه باید **Private IP** کامپیوتر **NAT Server** را به عنوان **Default gateway** خود واردکنند و آدرس **DNS** آنها باید آدرس **DNS server** اصلی شبکه باشد.
- بر روی همه ی کارت های شبکه ی درگیر **NAT**، نباید قابلیت **NLB** فعال باشد. (چه در **Client** ها و چه در **RRAS**)
- برای برخی اعضای شبکه، مثل **Web Server** ها، باید دو کارت شبکه تهیه شود، یکی برای قابلیت **NLB** و دیگری برای کارهای معمول شبکه که اتصال به **NAT Server** برای آن ضروری است.
- در حقیقت در **Dynamic NAT**، ما تمام یک شبکه (یا یک **Subnet** از یک شبکه) را به یک شبکه ی دیگر (یا یک **Subnet** دیگر از همان شبکه) متصل می کنیم.

می خواهیم شکل زیر را راه اندازی کنیم:
طوری که همه ی **Client** های متصل به شبکه ی **DC1**، مثل **PC1**، به **Webserver1** دسترسی داشته باشد.



در حقیقت این شبکه را بطور آزمایشی پیاده سازی می کنیم، اما در واقعیت، تنظیمات **IP** ای که برای **NIC** دوم **Nat Server** انجام داده ایم، مثل **Public IP** ای است که خریداری کرده ایم؛ و **Webserver1**، در دنیای **Internet** قرار دارد.
در این مثال، برای **Web Server** می توان یک سیستم **Client** را با یک ویندوز معمولی، قرار داد.

1. کنسول **RRAS** را بر روی **NAT Server** راه اندازی می کنیم.
   - در بخش **Role Services**، گزینه ی **Routing** را انتخاب می کنیم و تا پایان نصب پیش می رویم.
   - از منوی **Tools**، وارد گزینه ی **Routing and Remote Access** می شویم.
   - حال اگر در کادر سمت چپ این کنسول، آبجکت **Server** موجود نبود، بر روی **Routing and Remote Access** کلیک راست و **Add Server** و سپس **the Following Computer** را زده و نام **FQDN** این سرور را درج و **OK** می کنیم.
   - بر روی سرور اضافه شده، کلیک راست کرده و **.Configure and enable Rout** را می زنیم.
   - گزینه ی دوم یعنی **NAT** را انتخاب می کنیم.
   - در تب **NAT Internet Connection** آداپتوری که به اینترنت (شبکه ی خارجی) (**23.1.2.101**) وصل است را می زنیم.
   - در تب **Network Selection** آداپتوری که به شبکه ی داخلی وصل است را انتخاب می کنیم.(**192.168.139.147**) و **OK**!
   - حال اگر وارد زیرگزینه های آبجکت **Server** و سپس **IPv4** شویم، **NAT** را می بینیم که درونِ آن، آداپتورها اضافه شده اند.

نکته: اگر قصد داشتیم که خود DC1 را به عنوان NAT استفاده کنیم، تا همینجا کافی بود، و به سادگی NAT ایجاد شده بوده است.

2. یک Static Route برای DC1 تعریف می کنیم.

- برای دیدن همه ی Route های جاری سیستم، در PowerShell درج می کنیم:

```
Get-NetRoute -AddressFamily IPv4
```

- همانطور که می بینیم، وقتی مقصد یک Packet، ناشناس یا نامشخص برای شبکه ی جاری باشد، آنرا با آدرس 0.0.0.0 به مقصد Router یا Router های تعریف شده برای آداپتور ارسال می کند.
نکته ی موردنیاز این جدول، شماره ی ifindex مربوط به شبکه ی داخلی است؛ که به آن نیاز داریم.
- برای تعریف یک Route جدید، درج می کنیم:

```
New-NetRoute -DestinationPrefix 23.1.2.0/24 -InterfaceIndex 8 -NextHop 192.168.139.147
```

- همانطور که می بینیم، مقدار interfaceIndex همان ifindex مربوط به آدرس های داخل شبکه است.
- این دستور تعیین می کند که هرگاه درخواستی برای شبکه ی 23.1.2.0 آمد، آن را به سوی سیستم NAT Server بفرست.
- حال به سادگی می توان از هریک از Client های شبکه ی داخلی، مثل PC1 ، به IP مربوط به Webserver1 پینگ و مشاهده کرد که اتصال برقرار است.
- اگر در Webserver1 سرویس IIS را نصب و Implementation کرده باشیم، می توانیم در Client های داخلی شبکه و در مرورگرها، آدرس IP سیستم Webserver1 را وارد کنیم تا صفحه ی مربوط به IIS را نیز مشاهده کنیم.

نکته: برای قطع موقتی ارتباط میان دو شبکه ی داخلی و خارجی توسط NAT، کافی ست در کنسول Routing and Remote Access روی آبجکت Server کلیک راست کرده و در All Tasks گزینه ی Stop را بزنیم و برای اتصال مجدد، گزینه ی Start را!!

نکته: اما اگر به جای شبکه ی 23.1.2.0 می خواستیم، فقط شبکه ی داخلی را توسط NAT Server به اینترنت متصل کنیم، به جای مرحله ی دوم، کافی می بود که در DHCP Server شبکه، برای Scope Option گزینه ی Router 003 را روی آدرس 192.168.139.147 قرار دهیم.

برای حذف Route :

```
Remove-NetRoute -DestinationPrefix 23.1.2.0/24 -InterfaceIndex 8 -NextHop 192.168.139.147
```

Ports :

DNS : Port 53 :

پورت 53 برای سرویس DNS استفاده می شود، اما این سرویس از پورت های TCP و UDP این شماره، برای مصارف متفاوت استفاده می کند. از پورت TCP آن، برای انجام فرآیند Zone Transfer بین DNS Server ها و از پورت UDP آن برای Query گرفتن توسط کاربران (Name Resolution) استفاده می شود.

اگر یک مهاجم، سرور مقصد را اسکن کند و مشاهده کند که پورت TCP شماره 53 باز است به این معناست که این سرور، توانایی Zone Transfer را دارد و در واقع Database این DNS Server با چند DNS Server دیگر تبادل می شود.

توجه کنید که این ارتباط فقط میان DNS Server ها انجام می شود.

DNS Server ها همیشه برای Zone Transfer از پورت TCP استفاده می کنند.

برای اینکه فرآیند DNZ Zone Transfer بین دو یا چند DNS Server به درستی انجام شود، ارتباط بین DNS Server ها (چه مبدا و چه مقصد) باید با انجام تاییدیه های TCP یا همان TCP ACK انجام شوند.

اگر مهاجمی بتواند یک DNS Server جعلی راه اندازی کند و درخواست Zone Transfer به DNS Server واقعی بدهد، می تواند اطلاعات بسیار زیادی در خصوص کلیه رکوردهای موجود در DNS Server در فرآیند Enumeration بدست بیاورد.

NetBIOS : Port 137 :

همانطور که می دانید سرویس NetBIOS یک سرویس داخل شبکه ای برای تبدیل کردن اسم به آدرس IP و برعکس است که همچنین در شبکه های داخلی مورد استفاده قرار می گیرد، هر چند از نظر Microsoft منسوخ شده به حساب می آید.

Server این سرویس به عنوان WINS شناخته می شود که مخفف کلمه های Windows Internet Name Service است و بر روی پورت 137 پروتکل TCP فعال است.

همانند سرویس DNS سرورهای NetBIOS یا WINS دارای یک پایگاه داده یا Database هستند که در آنها آدرس های Host ها در کنار آدرسهای IP آنها نوشته شده است و در واقع وظیفه اصلی این سرویس، تبدیل کردن همین اسامی به آدرس ها و برعکس در پاسخ به Query کاربران است.

- برای مشاهده ی این Database :

nbtstat -c

- برای مشاهده ی Client های شبکه:

nbtstat -n

- برای حذف این Database:

nbtstat -r

این سرویس در شبکه های داخلی جزو اولین سرویس هایی است که مورد حمله مهاجمین در فرآیند Enumeration قرار می گیرد و با توجه به مکانیزم کاری که بر اساس Broadcasting انجام می شود، براحتی مورد حمله قرار گرفته و پایگاه داده خود را در اختیار مهاجم قرار می دهد.

پس در حملات درون شبکه ای، اولین سرویسی که معمولاً مورد حمله قرار می گیرد WINS یا NetBIOS است.

: NetBIOS Session Service : Port 139

سرویس NetBIOS Name Service با سرویس NetBIOS Session Service متفاوت است و حتی بر روی دو Port متفاوت کار می کنند.
سرویس NetBIOS Session Service برای ایجاد کردن Session بین کامپیوترهایی که از پروتکل NetBIOS پشتیبانی می کنند، استفاده می شود.
Session ها بین کامپیوترها با استفاده از ارسال Packet ایجاد می شوند.
کامپیوتری که قرار است Session ایجاد کند، برای کامپیوتر مقصد، درخواست خودش را بر روی پورت 139 ارسال می کند.
اگر Connection یا ارتباط برقرار شود ، کامپیوتر مبدا بر روی Connection ایجاد شده یک Session Request یا درخواست Session ارسال می کند، که این بسته ی Session Request به همراه NetBIOS Name نرم افزاری است که درخواست Session را داده است.
کامپیوتر مقصد برای اینکه ارتباط بصورت کامل برقرار شود، یک Positive Session Response برای ایجاد Session یا یک Negative Session Response به معنی عدم برقراری ارتباط، ارسال خواهد کرد.
به زبان ساده تر ابتدا یک Session بین کامپیوترهایی که از پروتکل NetBIOS Session Service استفاده می کنند برقرار می شود، پس از برقراری ارتباط Service یا Application ای که قرار است توسط این Session ارتباط را برقرار کند، درخواستی را ارسال می کند.

یک مهاجم می تواند با ایجاد کردن درخواست ها و Session های جعلی توسط نرم افزارهای مختلف، اطلاعاتی در خصوص نحوه ی عملکرد سرویس و ... از سیستم مقصد به دست بیاورد و این در واقع همان NetBIOS Session Service Enumeration می باشد.
دقت کنید ما SMB Over NetBIOS را عنوان کردیم، یعنی از این ارتباط در نهایت می توان برای ارسال و دریافت فایل استفاده کرد.

:(Server Message Block) SMB : Port 445

یکی از معروفترین پروتکل ها برای مدیریت اشتراک گذاری فایل و ارتباطات شبکه ای می باشد.
با استفاده از پورت 445 از نوع TCP ، می توان بصورت مستقیم و بدون استفاده از لایه واسط NetBIOS Session Service ، به کامپیوتر مقصد متصل شد و به همین دلیل که بصورت مستقیم و بدون واسطه، ارتباط را برقرار می کند به آن Direct Host نیز گفته می شود.

کاربرد اصلی آن انتقال فایل و استفاده از چاپگر در داخل شبکه است. توسط این پروتکل می‌توان منابعی که فایل‌ها را به اشتراک گذاشته‌اند و همچنین Client ها را مدیریت کرد.

: SNMP : Port 161

همانطور که می دانید پروتکل SNMP یک پروتکل مانیتورینگ و مدیریتی در شبکه محسوب می شود که هم در سیستم عامل ها و هم در تجهیزات و حتی Application های شبکه مورد استفاده می گیرد و اطلاعات مختلفی از اتفاقاتی که برای نرم افزار یا سخت افزار رخ می دهد را برای سرویس های مانیتورینگ ارسال می کند.
نرم افزارهای مانیتورینگ بسیاری هستند که ملاک کار آنها بر اساس SNMP می باشد.
معمولاً Agent های SNMP بر روی پورت 161 UDP کار می کنند، اما از همین Port و توسط String های پیشفرض و حمله به string های مورد استفاده در این پروتکل می توان اطلاعات ارزشمندی در مورد سیستم هدف پیدا کرد و همچنین می توان اگر قابلیت SNMP Write بر روی هدف فعال شده باشد، گاهی مدیریت هدف را نیز تا حدودی در دست گرفت.
SNMP ابزار بسیار مفیدی برای مهاجمین است.

: LDAP : Port 189

پروتکل LDAP مخفف کلمه های Lightweight Directory Access Protocol است و در واقع می توان از آن به عنوان پایگاه داده بسیاری از سرویس های احراز هویتی استفاده کرد.زمانیکه اسم پایگاه داده می آیند شما حتما باید مد نظر داشته باشید که حتما زبانی برای Query گرفتن یا پرس و جو از این پایگاه داده باید وجود داشته باشد.

LDAP بصورت مستقیم در سرویس هایی مثل Active Directory و سرویس های Email و ... استفاده می شود و همین مورد باعث می شود که مهاجم بتواند با برقراری ارتباط از طریق پروتکل LDAP بر روی پورت 389 بتواند اطلاعات مهمی از جمله نامهای کاربری و نام گروه ها و بسیاری از Contact هایی که در مجموعه ها وجود دارند را Enumerate کند.

سرویس Exchange Server و همچنین سرویس NetMeeting از جمله سرویس هایی هستند که به وسیله LDAP با Active Directory ارتباط گرفته و این سرویس را نصب و استفاده می کنند.

: Global Catalog : Port 3368

سرویس Global Catalog از پورت 3368 بصورت UDP و TCP استفاده می کند.

زمانیکه ما از یک پروتکل بصورت TCP یا Connection Oriented استفاده می کنیم در واقع نیازمند انجام شدن TCP Handshake هستیم که یک فرآیند سه مرحله ای برای اطمینان از درست دریافت شدن اطلاعات در مقصد است، می باشیم.

بعد از اینکه ارتباط برقرار شد می توانیم داده های خودمان را در Session ای که توسط TCP ایجاد شده است، ارسال کنیم و TCP به ما گارانتی می دهد که بسته های اطلاعاتی را به مقصد خواهد رساند.

اما اگر از پورت UDP استفاده کنیم، گارانتی یا تضمینی برای رسیدن بسته ی اطلاعاتی به مقصد نمی باشد و ممکن است در مسیر ارتباطی، برخی بسته ها اصلا به مقصد نرسند.

اگر بر روی سروری پورت شماره ی 3368 باز بود به معنی وجود سرویس Global Catalog و البته به معنی استفاده کردن از Windows Server و همچنین سرویس AD است و در صورت نیاز، مهاجم می تواند از این پورت برای بدست آوردن اطلاعات مربوط به Object های موجود در Directory Service استفاده کند.

: SMTP : Port 25

این پروتکل وظیفه ی انتقال Email در شبکه ی داخلی و اینترنت را بر عهده دارد و بر روی یک ساختار TCP با شماره پورت 25 فعالیت می کند.

اگر می خواهید تست کنید که پورت 25 بر روی Server مقصد شما باز است، براحتی می توانید بر روی پورت مورد نظر Telnet کنید.

این تکنیک معمولا برای تست کردن mail Server ها استفاده می شود، اما بطورکلی برای Test و Port Scan هم قابل استفاده است.

SMTP نیز یکی از سرویس هایی است که در فرآیند Enumeration می تواند استفاده شود و توسط آن می توان ساختار Email ID و گاهی بسیاری از نامهای کاربری را در شبکه ی مقصد Enumerate کرد.

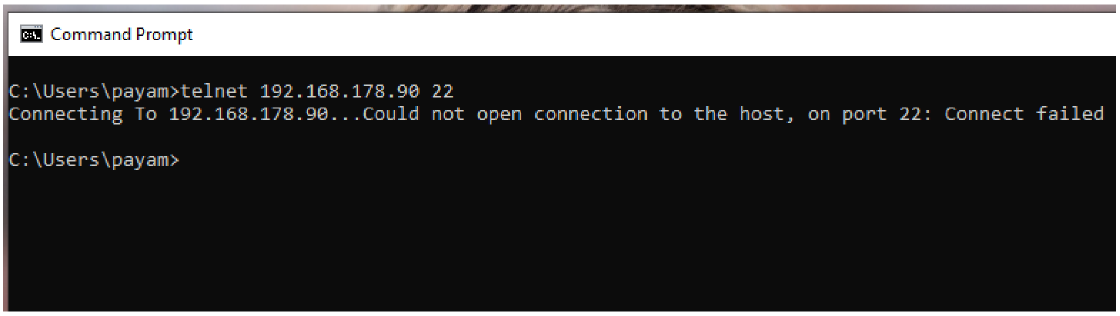
از Port های دیگر و Service های دیگری که در حوزه ی Email استفاده می شوند می توان از IMAP و POP نام برد، اما این پروتکل ها از درجه ی امنیتی بالاتری برخوردار هستند و امکان Enumerate کردن در آنها بسیار ضعیف است.

: Port verification

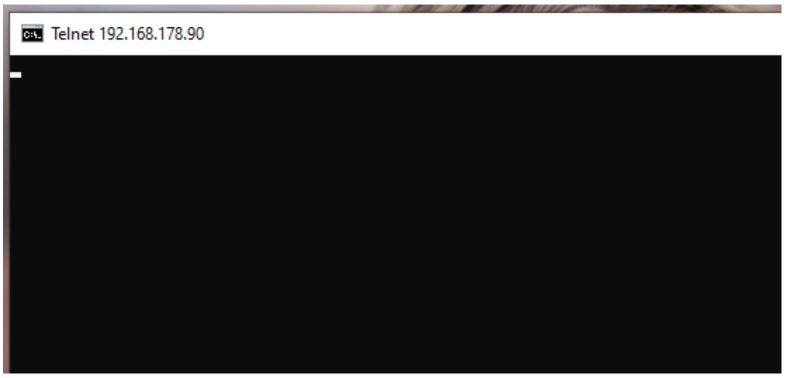
برای بررسی اینکه یک Port روی یک سیستم باز یا بسته است، نیاز به ابزار دستوری Telnet داریم.
با فرض اینکه این پروتکل روی سیستم فعال است، وارد cmd شده و به کمک آدرس یا نام سیستم موردنظر (یا سیستم جاری)، Port موردنظر را بررسی می کنیم (مثلن پورت remote desktop که 3389 می باشد.):

telnet 192.168.178.90 3389

اگر در پاسخ، خط زیر ظاهر شد، یعنی آن Port روی آن مقصد، بسته است:



اگر به جز یک خط نشان چشمک زن، چیزی ظاهر نشد، یعنی آن Port روی آن مقصد، باز است:



نکته: نرم افزارها و Application های زیادی جهت چک کردن Port های یک مقصد موردنظر وجود دارند، که این کار را به سادگی و سریع انجام می دهند.

در **PowerShell** هم، یکی از قابلیت های منحصربفرد دستور Test-NetConnection ، تست **Port** یا **Port** های مقصد است.

- **بررسی ارتباط با پورت http روی سایت blogfa.com:**

```
Test-NetConnection blogfa.com -CommonTCPPort http
Test-NetConnection blogfa.com -Port 80
```

و در پایان، در نتیجه ی ظاهر شده، اگر در مقابل گزینه ی TcpTestSucceeded عبارت **True** درج شده باشد، آن پورت باز و قابل دسترس است، و اگر False درج شده باشد، آن پورت بسته و غیرقابل دسترس می باشد.

- **Port List Scan: جهت بررسی باز یا بسته بودن همزمان یک سری Port های موردنظر، روی یک Server مقصد، طوری که نتایج، به شکل مجزا و مشخص نمایش داده شوند، می توان از Script زیر استفاده کرد** (در اینجا مثلاً google.com):

```
$ports = 22, 53, 80, 445, 443, 3389
$ports | ForEach-Object {
    $port = $_; if (Test-NetConnection -ComputerName www.google.com -Port $port -InformationLevel Quiet
-WarningAction SilentlyContinue)
    {
    "Port $port is open" }
    else {
    "Port $port is closed" } }
```

نکته:

- دلیل استفاده از InformationLevel Quiet ، اعلام به عدم نیاز به ظاهر شدن کلیه ی جزییات نتیجه است.
- دلیل استفاده از WarningAction SilentlyContinue این است که، در حالت عادی، اگر یک Port روی مقصد، بسته باشد، یک پیغام خطای نارنجی رنگ دریافت می کنیم، که با این سوییچ، از ظاهر شدنِ آن، جلوگیری می کنیم.

- **Port Range Scan: جهت چک کردن کلیه ی Port ها در یک محدوده، بر روی یک Server مقصد، بطور همزمان و با نتیجه ی مجزا و مشخص، می توان از Script زیر استفاده کرد** (در اینجا مثلاً google.com):

```
$destin = Read-Host "The destination  hostname  or  IP address  please"
[int]$i1 = Read-Host "Begin of the range please"
[int]$i2= Read-Host "End of the range please"
++$i2
        while ($i1 -lt $i2) {
        if (Test-NetConnection $destin -Port $i1 -InformationLevel Quiet -WarningAction SilentlyContinue)
        {
        "Port $i1 is open" }
        else {
        "Port $i1 is closed" }
                    ++$i1
                    }
```

نکته: درحقیقت دستور Test-NetConnection وقتی پورتی که در مقصد بسته است را چک می کند، مدت زمان زیادی را صبر می کند، که این درنگ، برای Port Range Scan زمانبر و طاقتفرساست.

➢ **برای مشاهده ی پورت های در حال استفاده در سیستم جاری و پورت هایی که جهت ارتباط با مقصد، از آنها استفاده می شود، به شکل Admin وارد CMD شده و:**

netstat -aon

- می بینیم که در نتیجه، هریک از اتصال ها، دارای یک شماره به نام Process Identifier یا همان PID می باشد؛ که جهت یافتن سرویس یا نرم افزار مربوط به آن، کافی ست وارد کنسول Task Manager شده و در ستون PID آن را جستجو کرد.
- شماره پورت در زیر ستون Local Address نمایش داده می شود. مثلن اگر آدرس برای Local به شکل 0.0.0.0:5040 باشد، 5040 در اینجا شماره پورت است.

➢ **برای مشاهده ی همه ی Port های سیستم، در cmd از دستور زیر استفاده می کنیم :**

netstat -na | find "یک شماره یا عبارت موردنظر"

با استفاده از این دستور تمام Port های فعال TCP و UDP که Packet ها را ارسال می کنند، مشخص می شوند.

➕ **راهکار ساده تر و حرفه ای تر جهت تست و بررسی Port های باز روی یک کامپیوتر، استفاده از نرم افزارهای کمکی است.**

To Open/Close a Port :

در **Run** تایپ می کنیم: **wf.msc**

- **Inbound** مربوط به ترافیکی است که از خارج، وارد می شود؛ و **Outband** مربوط به ترافیکی است که از داخل، خارج می شود.

در سمت چپ، برروی **Outband Rules** و یا **inbound rules** راست کلیک کرده و گزینه ی **New Rule** را انتخاب کنید.
در صفحه باز شده گزینه **port** را انتخاب کرده و روی **next** کلیک کنید.
در صفحه باز شده در قسمت **specific local ports** پورت یا پورت های مد نظر خود را نوشته و روی **next** کلیک کنید.

برای بستن Port :

در صفحه بعد گزینه **block the connection** را انتخاب کرده روی **next** کلیک کنید.

برای باز کردن Port :

در صفحه بعد گزینه **allow the connection** را انتخاب کرده روی **next** کلیک کنید.

دوباره روی **next** کلیک کنید.
در این صفحه در قسمت **name** یک نام دلخواه وارد کرده و روی **finish** کلیک کنید.

برخی از بد افزارها، قابلیت باز کردن بی اجازه ی پورت های سیستم های مقصد را دارند، که راه را برای حمله و هک باز می کند.
نرم افزاری به نام **Nmap** یا **Zenmap** وجود دارد که با درج و اسکن کردن **IP** مقصد، می توان بررسی کرد که در آن سیستم چه **Port** هایی باز هستند.

: Port Forwarding

ما در خانه هایمان از یک **Modem** استفاده می کنیم و موبایل ها و کامپیوترهای ما پشت این مودم قرار دارند و از بیرونِ شبکه قابل دسترسی نیستند.

ما با انجام **Port Forwarding** می توانیم دسترسی به **Client** های داخلیِ شبکه را از محیط بیرون (مثل **Internet**)، ممکن کنیم.

پس **Port Forwarding** درخواست های دریافتی از شبکه های خارجی را، به مقصد مشخص شده در شبکه ی داخلی هدایت می کند.

کاربرد های **Port Forwarding** :

- اتصال به دوربین های مدار بسته ی یک محیط، از راه دور
- راه اندازی یک **Web Server** عمومی
- دسترسی خصوصی و از راه دور به یک **Web Server** خصوصی
- دسترسی امن و از راه دور به شبکه ی **Local** بر روی شبکه اینترنت
- دسترسی امن به شبکه ی **Local** توسط پروتکل **FTP** برای انتقال فایل

نیازمندیها جهت انجام **Port Forwarding** در محلی که قرار است به آن متصل شویم:

- **Router** باید قابلیت **Port Forwarding** را داشته باشد.
- **Router** باید دارای یک **Static IP Address** باشد که این آدرس از طریق **ISP** تامین خواهد شد.
- هر سیستم یا دوربین و یا هر **Client** ای که به **Router** متصل است، آدرس **Local** و **Port** مجزا داشته باشد.

فرض کنید:

سازمان شما دارای یک **Web Server** است و نیاز دارید که از بیرون شبکه به این **Server** با استفاده از **Remote desktop** وصل شوید.

از طرف دیگر سازمان دارای دو دوربین مدار بسته است که جهت نظارت بر سازمان، در دو نقطه ی مختلف قرار گرفته‌اند.

Server و دوربینها به طور مستقیم یا غیرمستقیم با **Router** در ارتباط هستند.

یکی از راه های ممکن، خرید و اختصاص یک **Public IP** به **Server** و یا به دوربین موردنظر است.

- در این روش نیازی به **Port Forwarding** نیست و از بیرونِ شبکه با استفاده از **Public IP** می‌توان به سیستم مربوطه و یا به دستگاه مربوطه، دسترسی داشت.
- اما این راهکار از نظر هزینه و امنیت، مقرون به صرفه نیست، چون هر آدرس **Public** هزینه دارد و به سادگی هرکسی می تواند به **Client** ها دسترسی داشته باشد.

Router Port Forwarding :

فرض کنید شما دارای یک **Public Address** هستید که توسط **ISP** به **Router** اختصاص یافته است.
اما علاوه بر این **Public Address**، باید **Port** های دستگاههای موجود در شبکه ی داخلی نیز تنظیم شوند، تا برای ارتباط از راه دور با آنها، **Modem** قادر به شناسایيِ درخواست های آمده و ارسال آنها به هریک از **Client** ها باشد.

با توجه به سناریوی بالا نیاز داریم که پورت های
3389 (مربوط به **Remote Desktop**) ،
80 (مربوط به **Web** یا همان **HTTP**) ،
و بطور مثال دو پورت به شماره های **1000** و **1001** را برای **Public Address** ای که داریم، **Forward** کنیم.

هر درخواستی که به **Modem** می رسد، باید با توجه به **Port** مقصدی که برایش تعیین شده است، به سرویس یا **Device** مربوط به آن، در داخل شبکه ی داخلی، **Forward** شود.
IP های **Client** های شبکه مان، به صورت زیر می باشند:

Web Server : 192.168.1.10
Camera 1: 192.168.1.20
Camera 2: 192.168.1.30

پس فقط نیاز است که این تنظیمات را روی **Modem** انجام دهیم:
پورت های **80** و **3389** را به آدرس 192.168.1.10 و پورت های **1000** و **1001** را به ترتیب به آیپی های 192.168.1.20 و 192.168.1.30 **Forward** کنیم.

1. **برای انجام Port forwarding به صفحه ی User Interface مودم می رویم.**

تنظیمات پیکربندی **Port Forwarding** بطور معمول در بخش **NAT** و سپس در قسمت **Server** های مجازی یا **Virtual Servers**، قابل مشاهده هستند.

در پایان برای مشاهده ی تصاویر دوربین ها از راه دور، مثلاً اگر **Public IP** ما برابر با **88.23.54.111** باشد:
باید در **Remote Browser** خود، آدرس **88.23.54.111:1001** را برای دسترسی به **Camera 2** وارد کنیم.

نکته: اگر هنوز هم نمی توانید تصویر دوربین را از راه دور مشاهده کنید، مراحل زیر را طی کنید:

- در **Control Panel** وارد **Internet Options** شوید.
- در صفحه ی باز شده وارد قسمت **Security** شوید.
- بر روی **Custom Level** کلیک کنید.
- در صفحه ی باز شده، دو گزینه ی زیر را پیدا کرده و گزینه ی **Prompt** در زیر آنها را فعال کرده و **Ok** کرده و خارج شوید:
  - **Download Unsigned ActiceX Controls**
  - **Initialize and Script ActiveX Controls not marked as safe for script**

فرض کنید می خواهید یک وبسایت که در **Server** محل کارتان است را روی اینترنت قرار دهید، یا می خواهید به **Server** شبکه، از طریق اینترنت **Remote Desktop** کنید، و یا توسط **VPN**، به **Server** متصل شوید.

برای **Remote Desktop** باید **Port Forwarding** را طوری تنظیم کنید که درخواستهایی که از خارج به پورت **3389** در مودم وارد می شوند را به پورت **3389** در **Server** ارسال کند.

برای درخواست های **VPN** به **Server**، باید پورت **1723** را در **Modem** به پورت **1723** در **Server** متصل کنید.

و مهم ترین نکته اینکه اگر بین **Modem** و شبکه ی شما **Firewall** هم قرار دارد، باید برای **Firewall** هم تعریف کنید که اگر درخواستی از **Port** های موردنظر از سمت **Modem** آمد، آن را به کجا بفرستد، در حقیقت همان **Port forwarding** را درون **Firewall** نیز باید تنظیم کرد. هر **Firewall**، قوانین و ویژگی های خاص خودش را دارد.

:Port Forwarding Types

: Local port forwarding

این یکی از متداولترین نوع Port Forwarding ها می باشد که به اصطلاح به آن SSH یا Secure Shell نیز گفته می شود.
در این روش کاربران از راه دور توسط Command Line قادر خواهند بود در حالت Secure، اقدام به انتقال اطلاعات بین برنامه ها و کامپیوترها و سرورها نمایند.
مثلاً برخی از سرویس ها هستند که فقط از طریق دسترسی Local امکان دسترسی به آنها ممکن می باشد و هرگونه دسترسی از راه دور به آنها توسط Firewall مسدود خواهد شد.اما از طریق Local Port Forwarding با استفاده از فراهم شدن خطی امن بر روی خط عمومیِ اینترنت (که نا امن محسوب می شود) کاربر قادر خواهد شد تا از راه دور به این منابع و سرویس های Local دسترسی پیدا کند.
به همین جهت برنامه های متعددی وجود دارند که به آنها SSH Client گفته می شود و شما می توانید برای برقراری یک ارتباط امن از راه دور، از آنها استفاده نمایید که یکی از معروفترین آنها Putty می باشد.

: Remote port forwarding

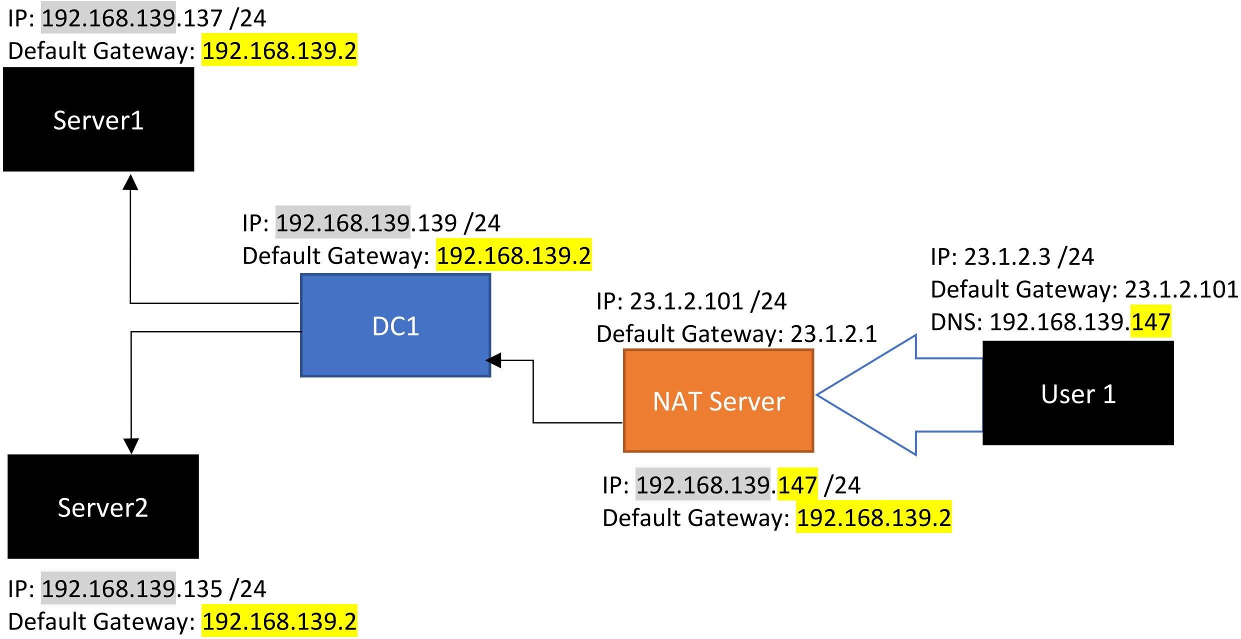
در این روش نیز با انجام برخی تنظیمات بر روی Router خود و Forward کردن پورت 3389 (همان پورتRemote desktop Protocol) به IP مقصدی که قصد اتصال از راه دور به آن را دارید، به راحتی می توانید در هر زمان و از هر مکانی به کامپیوتر تعیین شده ی خود متصل شوید.

: Dynamic port forwarding

در این حالت Port forwarding این امکان را برای کاربران شبکه های نا امن و عمومی فراهم می کند تا بتوانند اطلاعات و درخواست های خود را از طریق سروری امن رد و بدل نمایند.
معمولاً در اماکنی که از لحاظ امنیت بسیار ضعیف می باشند، کاربرد دارد، مانند کافی شاپ ها، هتل ها و ....

:Destination NAT (Microsoft Port Forwarding)

فرض کنید که در شبکه ی داخلی، چند **Server** داریم، که می خواهیم کاربران اینترنتی، به هریک از این **Server** ها دسترسی داشته باشند.
از طرفی هریک از این **Server** ها، یک **Member Server** هستند و یک **IP** مربوط به شبکه ی داخلی دارند.
پس باید برای اتصال به هریک از این **Server** ها، یک **Port** در **Router** و یا **NAT Server** این شبکه ی داخلی، تعریف کنیم.



1. **Server1** را تبدیل به یک **Web Server** می کنیم.

2. کنسول **RRAS** را بر روی **Implementation NAT Server** می کنیم.

- در بخش **Role Services**، گزینه ی **Routing** را انتخاب می کنیم و تا پایان نصب پیش می رویم.
- از منوی **Tools**، وارد گزینه ی **Routing and Remote Access** می شویم.
- حال اگر در کادر سمت چپ این کنسول، آبجکت این **Server** موجود نبود، بر روی **Routing and Remote Access** کلیک راست و **Add Server** و سپس **the Following Computer** را زده و نام **FQDN** این سرور را درج و **OK** می کنیم.
- بر روی سرور اضافه شده، کلیک راست کرده و **.Configure and enable Rout**را می زنیم.
- گزینه ی دوم یعنی **NAT** را انتخاب می کنیم.
- در تب **NAT Internet Connection** آداپتوری که به اینترنت (شبکه ی خارجی) وصل است را می زنیم. (**23.1.2.101**)
- در تب **Network Selection** آداپتوری که به شبکه ی داخلی وصل است را انتخاب می کنیم.(**192.168.139.147**) و **OK**!
- حال اگر وارد زیرگزینه های آبجکت **Server** و سپس **IPv4** شویم، **NAT** را می بینیم که درونِ آن، آداپتورها اضافه شده اند.

- بر روی **Ethernet1** یا همان آداپتوری که به شبکه ی **23.1.2.0** متصل است، کلیک راست کرده و **Properties** و سپس وارد تب **Services and Ports** می شویم.
- همانطور که می بینیم سرویس های زیادی وجود دارند، اما برای استفاده از سرویس های دیگر، **Add** را می زنیم.
- یک نام درج کرده و **on this interface** و **TCP** را انتخاب کرده و بقیه ی گزینه ها را بصورت زیر درج می کنیم و **OK**:

Incoming Port : مثلاً 6000
Private Address : 192.168.139.137
Outgoing Port : 80

3. یک Static Route ایجاد می کنیم.

- پس تا اینجا در **NAT Server** تعریف کردیم که اگر پیامی از بیرون برای کارت شبکه ی با آدرس **23.1.2.101** آمد، که به پورت **6000** درخواست داشت، آن را از طریق کارت شبکه ی با آدرس **192.168.139.147** به **Client** متصل به آن با آدرس **192.168.139.139** ارسال کن.
- اما از طرف دیگر، موقعی که سیستم **192.168.139.139** به پیام دریافتی از بیرون جواب می دهد، جواب از شبکه خارج نمی شود، پس باید یک **Static Route** برای ارسال پیام ها از طریق کارت شبکه ی **23.1.2.101** به بیرون ایجاد کنیم.
- پس به سیستم **DC1** رفته و در **PowerShell**:

ابتدا برای دیدن همه ی **Route** های جاری سیستم، درج می کنیم:

Get-NetRoute -AddressFamily IPv4

نکته ی موردنیاز این جدول، شماره ی **ifindex** مربوط به شبکه ی داخلی است؛ که به آن نیاز داریم.

1. برای تعریف این **Route**، درج می کنیم:

New-NetRoute -DestinationPrefix 23.1.2.0/24 -InterfaceIndex 8 -NextHop 192.168.139.147

4. نتیجه را test می کنیم.

- در حقیقت آدرس **User1** که یک کاربر خارجی است را نیز، همرنج با **NIC** دوم مربوط به **NAT Server** در نظر می گیریم.
- اگر وارد سیستم **User1** شده و به آدرس **Server1** یعنی **192.168.139.137** پینگ کنیم، جواب نمی دهد.
- اما اگر به **NAT Server** یعنی **23.1.2.101** پینگ کنیم، جواب می دهد.
- حال در همین سیستم **User1** وارد مرورگر **IE** یا **Chrome** شده و آدرس زیر را وارد می کنیم:

http://23.1.2.101:6000/

باید صفحه ی **IIS** مربوط به **Server1** را نشان دهد، که یعنی ما از بیرون یک شبکه، به یکی از **Server** های درون آن شبکه متصل شده ایم.

Remote Desktop and FTP with Microsoft NAT :

در حقیقت برای اینکه یک کاربر در یک شبکه ی دیگر و یا از راه دور بتواند به سیستم ها و **Server** های داخلی شبکه مان ارتباطات مختلفی مثل **FTP** و **Remote Desktop** برقرار کند، کاملاً به روش **Destination NAT** انجام می شود.
با این تفاوت که در تنظیمات **RRAS**، وقتی وارد تنظیمات **Ethernet1** یا همان آداپتوری که به شبکه ی بیرون متصل است، می شویم، در تب **Services and Ports**:
سرویس موردنظر را انتخاب و تنظیم کنیم، و یا روی **Add** زده و یک نام دلخواه و یک **Incoming Port** دلخواه و **Outgoing Port** متعلق به سرویس موردنظر را درج می کنیم، که این **Port** های مشخص برای سرویس ها ثابت هستند که یا باید در دسترس داشت یا باید حفظ کرد!

مثلاً برای **Remote Desktop** که البته گزینه ی آن از پیش تعریف شده است، می توان یک اتصال **Remote Desktop** دیگر هم برای یک سیستم دیگر تعریف کرد، پس باید وارد **Add** شده و مشخصات را تعیین و فعال کرد:
Incoming Port : مثلاً 6234
Private Address : 192.168.139.135
Outgoing Port : 3389
تنها گزینه ی مهم، شماره ی **Outgoing Port** است که برای **Remote Desktop** مقدار ثابت **3389** می باشد.

حال در یک سیستم بیرونی، برای اتصال به این سیستم داخلی دارای آدرس **192.168.139.135**، باید در **Remote Desktop**، آدرس را بصورت **20.1.2.101:6234** وارد کرد.

در حقیقت این تعیین کردن ارتباطات برای **NAT** را می توان از طریق **PowerShell** هم انجام داد، اما با این تفاوت که تمام ارتباطات **NAT** ای که از طریق **PowerShell** تعریف می شوند، در کنسول **RRAS** (که در قسمت **NAT** می باشند) درج نشده و دیده نمی شوند!

برای ایجاد یک ارتباط **Remote Desktop** از طریق **NAT** :

1. **در سیستم NAT Server یک مسیر NAT یا NETNAT ایجاد می کنیم و برایش تعریف می کنیم که بر روی کدام Network ID ایجاد شود:**

```
New-NetNat -Name myRD -InternalIPInterfaceAddressPrefix 192.168.139.0/24
```

2. **Port ها و IP های ورودی مقصد را مشخص می کنیم:**

```
Add-NetNatStaticMapping -NatName myRD -Protocol TCP -ExternalIPAddress 0.0.0.0 -ExternalPort 6000
-InternalIPAddress 192.168.139.139 -InternalPort 3389
```

برای مشاهده ی **NetNat** های ایجاد شده در سیستم، درج می کنیم:

```
Get-NetNat
```

برای حذف یک **NetNat** :

```
Remove-NetNat -Name myRD
```

برای حذف یک **NetNatStaticMapping** :

```
Remove-NetNatStaticMapping -NatName myRD
```

نکته: با حذف کردن NetNat قبلی، تمامی تنظیمات Nat که به صورت گرافیکی انجام داده بودیم، کاملاً از کار می افتند، مگر اینکه سرویس NAT را حذف و از نو نصب کنیم.

Print Server :

انواع استفاده از Printer در شبکه:

- اتصال مستقیم Printer به Server :
  - Driver دستگاه چاپگر، فقط روی خود کامپیوتر Server نصب و تنظیم می شوند.
  - تمامی داده هایی که باید چاپ شوند، باید ابتدا به Server منتقل شوند و سپس چاپ می شوند.

- اشتراک گذاری Printer متصل شده به Server :
  - فرض کنیم در روش قبلی، نقش Print Server را روی Server راه اندازی می کنیم، و Printer را Share کنیم.
  - حال بطور خودکار، Driver چاپگر به همه ی Client های شبکه منتقل و نصب می شود، و همه می توانند فایل های شان را به چاپگر ارسال کرده و چاپ کنند.
  - اما همچنان بار مدیریتی چاپگر، به دوش Server است.
  - برای شبکه هایی که دارای نیازهای چاپی کمی هستند، مناسب است.

- اتصال Printer به شبکه:
  - Printer مثل یک Client، توسط Switch، به بدنه ی شبکه متصل خواهد شد.
  - Printer باید دارای یک NIC باشد، که اگر بطورپیشفرض فاقد NIC بود، می توان برای آن یک NIC تهیه و متصل کرد.
  - پس Printer هم از DHCP، یک آدرس IP دریافت خواهد کرد.
  - در این روش، همه ی Client ها، دسترسی مستقیم به Printer دارند و همگی Driver چاپگر را بطور خودکار دریافت می کنند.
  - از معایب این روش این است که مدیر شبکه، مدیریتی بر درخواست ها و صف چاپ Printer نخواهد داشت.

- اشتراک گذاری Printer متصل شده به شبکه:

هنگامی که در یک شبکه، Printer های موجود، با یکدیگر یک مجموعه تشکیل داده و از طریق یک Server کنترل می شوند و کاربران می توانند با اتصال به آن Server، به یکی از آنها و یا به یک Printer خاص از آن مجموعه، دسترسی داشته باشند، به آن سیستم، Print Server می گویند.

- در واقع Print Server، کامپیوتر یا دستگاهی است که از طریق شبکه به یک یا چند Printer و تعدادی یا همه ی Client ها متصل شده و پس از دریافت فرمان Print از Client ها، آن را به Printer مناسب منتقل می کند.
- Fax Server نیز به همین شکل کار می کند.

:VPN (Virual Private Network)

اصولاً VPN یک شبکه ی خصوصی است که در یک شبکه ی عمومی مانند اینترنت، به صورت نادیدنی (ناشناس) بکار می رود و فقط اعضای خاصی را به عضویت می پذیرد.

- VPN مسافت را بی‌معنی می‌سازد،
- امنیت را بالا می‌برد،
- دردسرهای استفاده از پروتکل‌های مختلف را حذف می کند.

VPN دو کاربرد دارد:

بطور طبیعی، برای اینکه دو کامپیوتر بتوانند همدیگر را ببینند (به هم Ping شوند) و با هم ارتباطات دیگر را انجام دهند، باید در یک شبکه باشند، یعنی آدرس های IP آنها در یک Range کاملاً یکسان باشد.

اگر دو کامپیوتر در یک شبکه نباشند، و قادر به برقراری اتصال فیزیکی بین آنها نباشیم، دیگر مهم نیست که فاصله ی آنها به اندازه ی یک خیابان باشد، یا به اندازه ی یک قاره باشد، باید یک اتصال VPN بین آنها برقرار کنیم.

پس برای اینکه دو کامپیوتر از دو شبکه ی مختلف و یا بطور کل دو شبکه بطور کامل، بتوانند بدون اتصال فیزیکی، با یکدیگر ارتباط برقرار کنند، از نوعی تونل درون اینترنت استفاده می کنیم، که وقتی هردو طرف رابطه، به آن وارد می شوند، مانند این است که آنها را بصورت فیزیکی به یکدیگر وصل نموده ایم که می توانند به هم Ping شوند!

در این حالت، دو روش برای ایجاد شبکه ی VPN وجود دارد:
طراحی VPN Server توسط Windows Server:

تنظیم VPN در Router یا Router ها:
اگر در هر دو Router مبدا و مقصد، VPN را تعریف کنیم، یک Lan to Lan VPN را ایجاد کرده ایم.
در این حالت دو شبکه محلی با کمک تونل VPN و از طریق Internet با هم ارتباط برقرار می کنند طوری که کاربران هر شبکه ی محلی به منابع شبکه محلی دیگر، به عنوان عضوی از آن شبکه، دسترسی دارند.اگر فقط در Router یک سمت، VPN را تعریف کنیم، یک ارتباط Client-Lan VPN را ایجاد کرده ایم.

البته در این زمینه، نرم افزارهایی هم هستند که با وارد کردن مشخصات و اطلاعات ورود، هم اتصال VPN را برقرار می کنند، و هم صفحه ی کنترل از راه دور را باز می کنند، مثل Team Viewer که برای استفاده ی اداری، نیاز به خریداری Serial Number دارد، که هزینه ی بالایی دارد.

استفاده از ارتباط VPN ، طوری که شخص دوم، با مشخصات کامپیوتر شخص اول، وارد محیط اینترنت یا شبکه ی بزرگی که هر دو در آن قرار دارند، شود!
مثلاً کسی که در تهران است، با وصل شدن به کامپیوتر شخصی که در برلین است، وارد اینترنت شود، در نتیجه تمام کارهایی که در اینترنت انجام می دهد، از دریچه ی سیستم قرارگرفته در برلین، صورت می پذیرد.
سیستمی که در برلین قرار دارد، می تواند تعداد زیادی سیستم را از سراسر جهان به خود وصل کند تا آنها بوسیله ی سیستم خودش وارد اینترنت شوند.
هر سیستمی که به سیستم برلین وصل شده و وارد اینترنت شود، با آدرس IP آلمان و آدرس برلین خواهد بود.
این ارتباط، یک ارتباط Client-Lan VPN است.

هر کاربری که قصد اتصال به VPN Server را داشته باشد، باید دارای یک username و password مختص به خود باشد که در VPN Server در برلین، بطور اختصاصی برای او تعریف شده باشد.

- اتصال های VPN توسط رمزهایی که یک Protocol مخصوص برای مبدأ و مقصدِ رابطه تعیین می کند، انجام می شوند. به همین جهت عملیات Encryption و Decryption در هر دو طرف رابطه، اهمیت بالایی دارند.

برای امنیت Tunnel یا شبکه ی VPN در فضای عمومی اینترنت، یک پروتکل بکار می رود، که می تواند یکی از انواع زیر باشد:

1. PPTP (Point To Point Tunneling Protocol):
   - PPTP قدیمی ترین، سریع ترین و ساده ترین و کم امنیت ترین پروتکل برقراری ارتباط VPN است.
   - فاقد توانایی encrypt کردن Data های ارسالی ست، و Data Encryption را پس از انتقال مشخصات کاربران انجام می دهد.
   - این پروتکل فقط خود تونل VPN را امن نگه می دارد؛ چون مشخصات کاربری، بر روی یک لینک ایمن (secure link) تبادل نمی شوند.
   - از پروتکل TCP با پورت 1723 و پروتکل IP با پورت 47 استفاده می کند.

2. L2TP (Layer Two Tunneling Protocol) یا IKEv1 (Internet Key Exchange version 1):
   - L2TP/IPSec یک طراحی مشترک از مایکرسافت و سیسکو است.
   - L2TP/IPSec بسیار بسیار از PPTP ایمن تر است چون قبل از اینکه مشخصات کاربری را تحت شبکه منتقل کند، با استفاده از پروتکل IPSec ، جلسه ی بین Client و Server را ایمن سازی می کند.
   - در حقیقت یک کلید ارسالی به Client، توسط پروتکل IPSec و به عنوان PreShared Key رمزنگاری می شود.
   - در این روش دیگر هکرها قادر نخواهند بود در line بایستند و اطلاعات را شنود کنند.
   - یکی دیگر از قابلیت های این پروتکل، Mutual Authentication (احراز هویت متقابل) است که امکان احراز هویت دو طرفه را به ما می دهد، یعنی هم Server مشخصات کاربر را احراز هویت می کند، هم کاربر، Server را احراز هویت می کند؛ که باعث می شود تا سرور به هر درخواستی جواب ندهد.
   - نسبت به PPTP سرعت کمتری دارد.
   - از پروتکل UDP و پورت های 500 و 4500 و 1701 استفاده می کند.

3. SSTP (Secure Socket Tunneling Protocol):
   - در ویندوز سرور 2008 و بعد از آن، پروتکل جدیدی به نام SSTP توسط مایکروسافت معرفی شد.
   - وقتی از پروتکل های PPTP یا L2TP استفاده می کنیم، باید پورتهایی خاص را در Firewall باز کنیم. مثل IPSec و ... اما گاهی در شبکه ها، به دلایلی، پورتهای HTTP و TCP باز هستند، پس مسئول شبکه تصمیم می گیرد که پورتهای بیشتری را باز نکند، پس از پروتکل SSTP برای اتصال VPN استفاده می کند.
   - فقط برای محصولات Microsoft کاربرد دارد.
   - به این جهت که به صدور Certificate نیاز دارد، راه اندازی پیچیده تری دارد.
   - از پروتکل SSL و TLS برای رمزنگاری کردن ارتباطات استفاده می کند.
   - SSTP پروتکل بسیار ایمنی است، چون تا قبل از اینکه یک ارتباط SSL ایمن بین کلاینت و سرور برقرار نشود، مشخصات کاربری را در شبکه ارسال نمی کند.
   - به SSTP برخی اوقات PPP بر روی SSL نیز گفته می شود، به این معنی که با ترکیب مکانیزم های PPP و SSL با یکدیگر، SSTP ایجاد می شود.
   - از پروتکل TCP و پورت 443 و پروتکل HTTP و پورت 80 استفاده می کند.

4. IKEv2 :

از قابلیت های آن، Re-establishing (Reconnection) می باشد، به این معنی که برخلاف پروتکل های قبلی، در صورت قطع و اتصال مجدد، همه چیز در آخرین حالت باقی می ماند و می توان کار را ادامه داد و نیازی نیست تا همه چیز را از نو شروع کنیم! بسیار ایمن است و البته راه اندازی پیچیده ای هم دارد!

5. Open VPN :

قدرتمندترین و ایمن ترین پروتکل VPN است.
Implementation آن در Windows بسیار پیچیده است.
Open Source است.

به طور اصولی، شبکه های VPN را به دو دسته تقسیم می کنند:

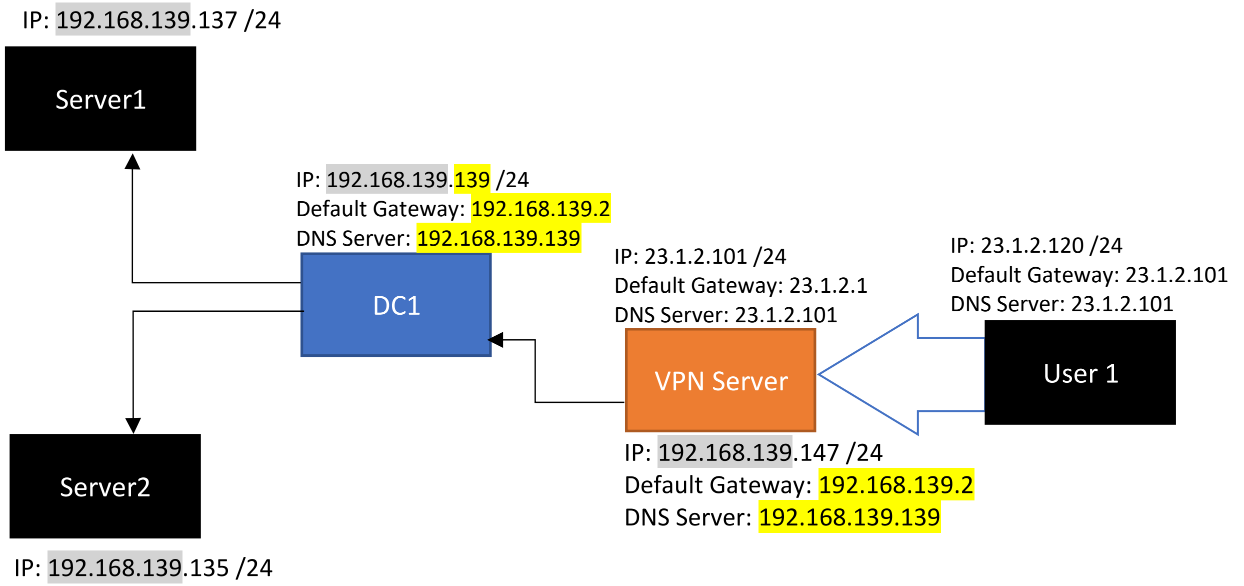
- RA (Remote Access) : که در یک طرف، یک VPN Server در یک شبکه نصب یا فعال می شود و در طرف دیگر، فقط نیاز به یک User Account و Password است، تا یک کاربر بتواند به آن شبکه متصل شود.
- S2S (Site to Site): جهت اتصال دو سایت یا دو شبکه ی متفاوت به یکدیگر بکار می رود.

VPN Requirements :

- یک سیستم احراز هویت کاربران (User Authentication): که توسط یکی از پروتکل های زیرانجام می شود: PAP ؛ CHAP ؛ MSCHAP و ...
- یک سیستم اختصاص آدرس IP (Address Assignment): علاوه بر DHCP Server می توان بصورت Static هم انجام شود.
- یک سیستم رمزنگاری (Data Encryption): که وابسته به پروتکل مورد استفاده است.
- پورت های مورد نیاز باز (Required Open Ports)
- سیستم های VPN Server باید در AD Users and Computers عضو گروه RAS and IAS Servers باشند.

Windows Connection Remote Access VPN :

فرض کنید دارای یک اینچنین شبکه ای هستیم، که یک کاربر در خارج از شبکه (**Internet**) قرار دارد و یک حساب کاربری به نام **User1** در **AD** برای آن ایجاد کرده ایم.



PPTP :

1. **VPN User ایجاد می کنیم.**

- به دو شکل می توان **VPN User** ایجاد کرد:
- روش اول:
  - درون **AD** یک **User** ایجاد می کنیم.
  - سپس وارد **Properties** این **User** شده و در تب **Dial-in**، برای قسمت **Network Access Permission** گزینه ی **Allow Access** را انتخاب کرده و **OK** کنیم.
- روش دوم:
  - در حقیقت می توان این **User** را در **VPN Server** هم به صورت یک **local Account** ایجاد کرد و همان را به عنوان **VPN User** استفاده کرد. البته برای این **User** هم باید در تنظیمات **local Users** وارد **Properties** آن شده و در تب **Dial-in**، برای قسمت **Network Access Permission** گزینه ی **Allow Access** را انتخاب کرده و **OK** کنیم.

2. **کنسول RRAS را بر روی VPN Server راه اندازی می کنیم.**

- ابتدا نقش **Remote Access** را با **Feature** های **Routing** و **DirectAccess and VPN** نصب می کنیم.
- وارد کنسول **Routing and Remote Access** می شویم.
- حال اگر در کادر سمت چپ این کنسول، آبجکت این **Server** موجود نبود، بر روی **Routing and Remote Access** کلیک راست و **Add Server** و سپس **the Following Computer** را زده و نام **FQDN** این سرور را درج و **OK** می کنیم.
- بر روی سرور اضافه شده، کلیک راست کرده و **Configure and enable Rout.** را می زنیم.
- گزینه ی اول یعنی **Remote access (dial-up or VPN)** را انتخاب می کنیم.
- گزینه ی **VPN** را انتخاب می کنیم.
- در تب **VPN Connection** آداپتوری که به شبکه ی خارجی وصل است را انتخاب می کنیم.(**23.1.2.101**) و **OK**!

- اگر گزینه ی .Enable Security on t را فعال کنیم، دیگر از محیط بیرون، قادر به Ping کردن به این سرور نخواهیم بود که بطورطبیعی بهتر است که در محیط عملی و واقعی، این گزینه را فعال نگه داریم. اما در محیط امن (مثل محیط تست و آزمایش) آن را غیرفعال می کنیم.
- در تب IP Address Assignment، باید تعیین کنیم که کاربرهایی که به VPN Server مان متصل می شوند، به چه شکل IP دریافت کنند.
- اگر Automatically را انتخاب کنیم، از DHCP Server شبکه داخلی مان آدرس دریافت می کنند، و اگر From a specified range را بزنیم، در تب بعد، باید یک محدوده از IP Address ها را درج و تعریف کنیم که از آنها، آدرس تخصیص بدهد.
- در تب Managing Multiple Remote Access Server، اگر بخواهیم که عملیات Authenticate کردن کاربران متصل به VPN، توسط یک Server جداگانه انجام شود، (Radius Server) در اینجا گزینه ی .. Yes, Set up را انتخاب می کنیم و Finish!

- برای انتخاب پروتکل احراز هویت VPN Connection ها در VPN Server، وارد Properties آبجکت Server شده و در تب Security وارد دکمه ی Authentication Methods می شویم و یکی یا تعدادی یا همه ی پروتکل ها را انتخاب می کنیم.

3. Network Policy را فعال می کنیم.

- در کادر سمت چپ، بر روی .Remote Access Logging کلیک راست کرده و Launch NPS را می زنیم.
- در پنجره ی باز شده، در سمت چپ آبجکت Network Policies را انتخاب کرده و در کادر سمت راست، وارد Properties گزینه ی .. Connections to Microsoft Routing and شده و گزینه ی ..Grant Access را انتخاب کرده و OK و یکبار سیستم را Restart می کنیم.

4. VPN Connection را در Client تنظیم می کنیم.

- در سیستم User1 آدرس IP و قابل Ping بودن به VPN Server را تست می کنیم.
- وارد Network and Sharing Center شده و گزینه ی Set up a new Connection or Network را می زنیم.
- Connect to a Workplace را و سپس (VPN) use my Internet connection را انتخاب می کنیم.
- در این مثال، چون Internet جدا برای این Client موجود نیست، گزینه ی .I'll set up an Internet Conn را می زنیم.
- حال برای Internet Address، آدرس بیرونی VPN Server، یعنی 23.1.2.101 را و یک نام برای آن، درج کرده و گزینه ی Remember my credentials را فعال کرده و Create و تمام!

- حال یا وارد Properties مربوط به VPN Connection ایجاد شده می شویم و در تب Security برای Type of VPN گزینه ی PPTP را انتخاب می کنیم و با انتخاب Allow these Protocols پروتکل هایی که برای Authentication Methods انتخاب کرده بودیم را فعال می کنیم و تمام!
- و یا بر روی آیکون کوچک مربوط به Network در سمت راست نوار Task Bar کلیک راست کرده و وارد Open Network and Internet Setting شده و در پنجره ی باز شده، از سمت چپ، وارد VPN Connection شده و روی گزینه ی VPN ایجاد شده در بالای کادر سمت راست، کلیک کرده و از زیرگزینه های آن، Advanced Options را زده و در پنجره ی جدید، Edit را می زنیم.

- در پایان برای استفاده از آن، کافی ست در همان پنجره ی Network and Internet Setting بر روی VPN ایجاد شده کلیک کرده و Connect را بزنیم و User و Password حساب کاربری که ایجاد کردیم را وارد می کنیم.

- اگر اتصال برقرار نشد، لازم است که یکبار سرویس RRAS را Restart کنیم.
پس بر روی آبجکت Server کلیک راست کرده و از گزینه های All Tasks گزینه ی Restart را می زنیم.
اگر باز هم ارتباط برقرار نشد، باید Server را کاملاً Restart کنیم.

حال بطورطبیعی می توانیم به همه ی Client های درون شبکه، Ping کرده و دسترسی داشته باشیم، مگر اینکه در VPN Server یک NIC سوم داشته باشیم، که مثلاً به یک اینترنت دسترسی داشته باشد و بخواهیم سیستم VPN Server دسترسی های کاربران خارجی را از خودش عبور داده و فقط به این اینترنت بدهد.

برای این کار در کنسول Routing and Remote Access بر روی آبجکت سرور کلیک راست کرده و Properties را زده و در تب IPv4، در پایین، گزینه ی Adapter را روی NIC سوم تنظیم می کنیم.

- هر کاربری که یک ارتباط VPN با این Server برقرار کند، در آبجکت Remote Access Clients درج خواهد شد.
- اگر وارد آبجکت Ports شویم، می بینیم که به تعدادی که می توان اتصال VPN با این Server برقرار کرد، پورت ایجاد شده است. برای کنترل تعداد مجاز برای ایجاد VPN با این Server، وارد Properties آبجکت Ports شده و نوع پروتکل موردنظر را انتخاب کرده و بر روی دکمه ی Configure زده و عدد دلخواهی برای تعداد موردنظر مقابل گزینه ی Maximum Ports درج می کنیم.
- برای تغییر روش اختصاص IP به کاربرهایی که توسط VPN متصل می شوند، وارد Properties آبجکت Server می شویم:
  - در تب IPv4 گزینه ی Enable IPv4 Forwarding را فعال می کنیم.
  - یا Dynamic Host Config. Protocol را می زنیم.
    - در پایین، برای Adapter، باید کارت شبکه ای را که مربوط به DHCP Scope موردنظر است را انتخاب کنیم.
    - حال اگر به DHCP Server و آن Scope برویم می بینیم که به تعداد 10 آدرس به این VPN Server، آدرس IP اختصاص داده است! سپس زمانی که این 10 آدرس اختصاص یابند، دوباره 10 آدرس دیگر به آن اختصاص می یابد.
  - و یا توسط Static address Pool به صورت دستی و دلخواه، یک Range تعیین می کنیم.
- در صورتی که بخواهیم هریک از User هایی که به VPN Server متصل می شوند، با یک IP مختص به خود وصل شوند، وارد تنظیمات Properties آن User شده و در تب Dial-in، آدرس IP آن را تعیین می کنیم.

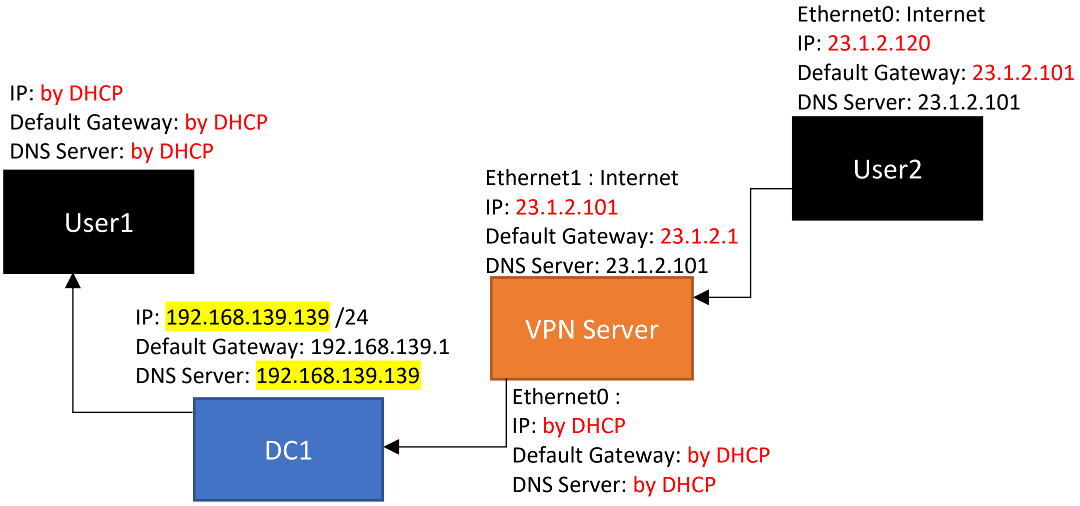
: L2TP

تمامی تنظیمات را مشابه با PPTP انجام می دهیم، به جز دو مورد زیر:

- وارد Properties مربوط به آبجکت Server شده و در تب Security گزینه ی ..Allow Custom Ipsec Policy for L2TP را فعال کرده و در نوار PreShared Key یک رمزعبور درج کرده و OK می کنیم.
- در سیستم Client وارد Properties مربوط به VPN Connection ایجاد شده می شویم و در تب Security برای Type of VPN گزینه ی L2TP/IPsec را انتخاب می کنیم و وارد دکمه ی Advanced Settings شده و use preshared key را فعال کرده و رمز عبوری که در RRAS وارد کردیم را در اینجا نیز درج می کنیم.

Connection Profile Remote Access VPN :

فرض کنید دارای یک اینچنین شبکه ای هستیم، که User2 یک کاربر در محیط خارج از شبکه (Intranet) است و می خواهد به شبکه متصل شود.



در حقیقت در مثال واقعی، IP مربوط به Ethernet1 در VPN Server باید Public Static IP و یا یک DDNS باشد.

1. کنسول RRAS را بر روی سرور VPN (VPN Server) راه اندازی می کنیم.

- وارد کنسول Routing and Remote Access می شویم.
- حال اگر در کادر سمت چپ این کنسول، آبجکت این Server موجود نبود، بر روی Routing and Remote Access کلیک راست و Add Server و سپس the Following Computer را زده و نام FQDN این سرور را درج و OK می کنیم.
- بر روی سرور اضافه شده، کلیک راست کرده و .Configure and enable Rout را می زنیم.
- گزینه ی اول یعنی Remote access (dial-up or VPN) را انتخاب می کنیم.
- گزینه ی VPN را انتخاب می کنیم.
- در تب VPN Connection آداپتوری که به شبکه ی خارجی وصل است را انتخاب می کنیم.(23.1.2.101) و OK!
- در محیط امن (مثل محیط تست و آزمایش) گزینه ی .Enable Security on t را غیرفعال می کنیم، اما در محیط عملی و واقعی، این گزینه را فعال نگه می داریم. (جهت عملیات Ping بکار می رود.)
- در تب IP Address Assignment، باید تعیین کنیم که کاربرهایی که به VPN Server مان متصل می شوند، به چه شکل IP دریافت کنند.اگر Automatically را انتخاب کنیم، از DHCP Server شبکه داخلی مان آدرس دریافت می کنند، و اگر From a specified range را بزنیم، در تب بعد، باید یک محدوده از IP Address ها را درج و تعریف کنیم که از آنها، آدرس تخصیص بدهد.
- در تب Managing Multiple Remote Access Server، اگر بخواهیم که عملیات Authenticate کردن کاربران متصل به VPN، توسط یک Server جداگانه انجام شود، که به آن سرور Radius Server گفته می شود، در اینجا گزینه ی .. Yes, Set up را انتخاب می کنیم و Finish!
- حال وارد Properties آبجکت VPN Server شده و در تب Security گزینه ی .Allow Custom Ipsec Po را فعال کرده و در نوار Preshared Key یک رمز عبور برای آن درج کرده و Apply و OK می کنیم.
- حال این آبجکت VPN Server را یکبار Restart می کنیم: All Task > Restart

2. تنظیمات VPN را درون یک Profile ایجاد می کنیم.

- در Server Manager و در Tools وارد گزینه ی Connection Manager Administration Kit می شویم.
- Windows Vista or above را می زنیم.
- New Profile را زده و سپس یک نام برای این سرویس و یک نام برای فایل خروجی (کمتر از 8 حرف) تعیین می کنیم.
- تنظیمات Realm و تنظیمات Merge را رها کرده و سپس تیک .Phone Book from را فعال کرده و در نوار .Always use آدرس IP مربوط به Ethernet1 خود VPN Server را وارد می کنیم.
- برای VPN Entry بر روی Edit زده و در تب Security برای اولین فهرست، گزینه ی .Only use Layer Two را انتخاب کرده و دکمه ی Advanced را زده و گزینه ی Use a Preshared Key را فعال می کنیم و در همان تب Security گزینه ی .Use Extensible Authentication را انتخاب و فهرست زیر آن را روی Microsoft:Secured Password (EAP-Mv2) تنظیم می کنیم و در زیر این فهرست، Properties را زده و گزینه ی .Automatically use my Windows log را فعال می کنیم. و می توانیم در تب General نوع ارتباط را بر حسب فقط IPv4 قرار دهیم و OK!
- دوباره Preshared Key را وارد می کنیم.همچنین برای زمانی که کاربر بخواهد این Profile را نصب و Implementation کند، یک Pin تعیین می کنیم.
- می توانیم بیشتر تنظیمات مثل و ...را رها کنیم.(مثلاً در Display Support می توان شماره تماس درج کرد.)
- در تب finish می بینیم که آدرس ذخیره ی فایل نهایی را نشان می دهد، پس آنرا کپی کرده و به آنجا رفته و پوشه ی نهایی که حاوی فایلهاست را کپی کرده و به User2 می بریم.
- حال فایل اجرایی را با دسترسی Admin باز کرده و Pin تنظیم شده را وارد کرده و نصب و اجرا می کنیم.

3. ارتباط را تست می کنیم.

- می توان در PowerShell مربوط به User2، دستور زیر را که مثل ipconfig /all بوده و مشخصات همه ی NIC ها را نشان می دهد، وارد کنیم:

```
Get-NetIPConfiguration
```

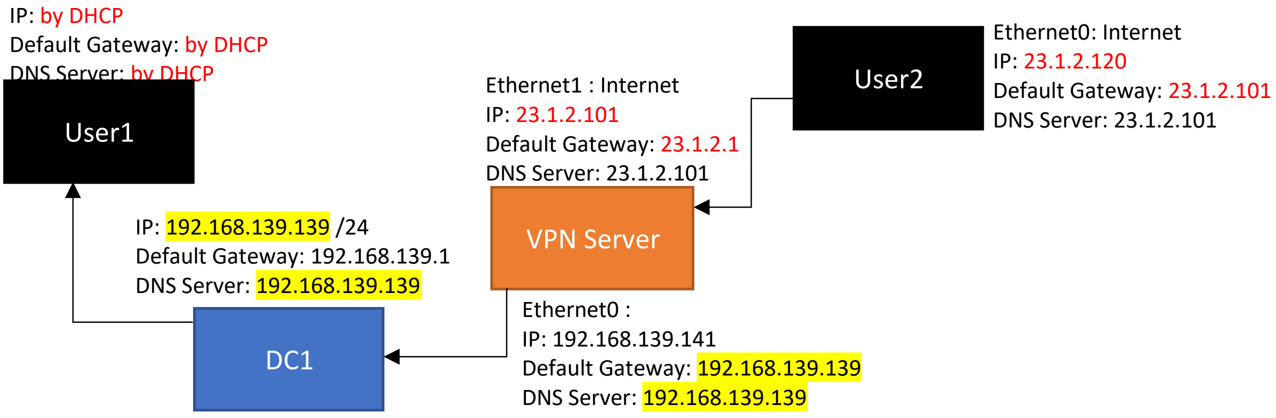
: IPv6 Remote Access VPN

در حقیقت VPN را ایجاد می کنیم، و در پایان:

1. در سیستم Client: وارد Properties مربوط به Profile Connection آن شده و به تب Networking رفته و گزینه ی IPv4 را غیرفعال کرده و IPv6 را فعال کنیم.
2. در VPN Server: به کنسول Routing and Remote Access رفته و وارد Properties آبجکت آن Server شده و در تب General گزینه ی IPv6 را فعال کرده و بر روی LAN and demand dial routing قرار داده و به تب IPv6 رفته و در نوار IPv6 Prefix عبارت Subnet prefix درنظر گرفته شده را درج می کنیم و در پایین همین تب Adapter رو به محیط خارجی را انتخاب می کنیم.

SSTP VPN:

فرض کنید دارای یک اینچنین شبکه ای هستیم، که User2 یک کاربر در محیط خارج از شبکه است و می خواهد به شبکه متصل شود.



- در حقیقت در مثال واقعی، IP مربوط به Ethernet1 در VPN Server باید Public Static IP یا DDNS باشد.
- در این پروتکل به دلیل امنیت بالا، نیاز به راه اندازی Certificate ها خواهیم داشت.
- در ابتدا بهتر است که اگر نقش NPS Server بر روی سرور VPN نصب است، آن را حذف کنیم.

1. VPN User ایجاد می کنیم.

- به دو شکل می توان VPN User ایجاد کرد:
- روش اول:
  - درون AD یک User ایجاد می کنیم.
  - سپس وارد Properties این User شده و در تب Dial-in، برای قسمت Network Access Permission گزینه ی Allow Access را انتخاب کرده و OK کنیم.
- روش دوم:
  - در حقیقت می توان این User را در VPN Server هم به صورت یک local Account ایجاد کرد و همان را به عنوان VPN User استفاده کرد. البته برای این User هم باید در تنظیمات local Users وارد Properties آن شده و در تب Dial-in، برای قسمت Network Access Permission گزینه ی Allow Access را انتخاب کرده و OK کنیم.

2. یک VPN Connection معمولی (PPTP یا L2TP) میان User2 و VPN Server راه اندازی می کنیم.

- نقش Remote Access را با Feature های Routing و DirectAccess and VPN نصب می کنیم.
- وارد کنسول Routing and Remote Access می شویم.
- حال اگر در کادر سمت چپ این کنسول، آبجکت این Server موجود نبود، بر روی Routing and Remote Access کلیک راست و Add Server و سپس the Following Computer را زده و نام FQDN این سرور را درج و OK می کنیم.
- بر روی سرور اضافه شده، کلیک راست کرده و .Configure and enable Rout را می زنیم.
- گزینه ی سوم یعنی VPN Access and NAT را انتخاب می کنیم.
- در تب VPN Connection آداپتوری که به شبکه ی خارجی وصل است را انتخاب می کنیم (23.1.2.101) و OK!
- در تب IP Address Assignment، باید تعیین کنیم که کاربرهایی که به VPN Server مان متصل می شوند، به چه شکل IP دریافت کنند.

- اگر Automatically را انتخاب کنیم، از DHCP Server شبکه داخلی آدرس دریافت می کنند، و اگر From a specified range را بزنیم، در تب بعد، باید یک محدوده از IP Address ها را درج و تعریف کنیم که از آنها، آدرس تخصیص بدهد.

- در تب Managing Multiple Remote Access Server، اگر بخواهیم که عملیات Authenticate کردن کاربران متصل به VPN، توسط یک Server جداگانه انجام شود، (Radius Server) در اینجا گزینه ی Yes, Set up .. را انتخاب می کنیم و Finish!
- و بقیه ی تنظیمات را انجام داده و اتصال VPN Remote Access را انجام می دهیم.

3. Certificate Authority Server را نصب و راه اندازی می کنیم.

- هم می توانیم در یک Server جدا آن را ایجاد و لینک کنیم، هم می توانیم در خود VPN Server آن را ایجاد کنیم.
- در اینجا، در خود VPN Server نصب می کنیم.
- مراحل نصب آن را از Add Roles And Features پیش می رویم.
- به این دلیل که ارتباط VPN تحت Web انجام می شود، در تب انتخاب Features، علاوه بر گزینه ی Certification Authority،
- Web Enrollment و Online Responder را نیز انتخاب می کنیم.
- در تب Select Role Services ، تمام زیرگزینه های گزینه ی Security را فعال می کنیم.
- اگر IIS نصب نبوده است، آن را نیز نصب می کنیم.

نکته: به User ای که با آن اقدام به نصب این Role می کنیم باید دقت کرد که حتماً Administrator باشد.

- در زمان Configure کردنِ آن، ابتدا فقط Certification Authority را برای Configure انتخاب می کنیم، و وقتی دوباره سوالی مبنی بر پیکربندی سرویس های دیگر می پرسد، yes را زده و اینبار هردوی دیگر را انتخاب می کنیم.
- آن را از نوع Enterprise و Root CA انتخاب کرده و گزینه ی Create a new private key را انتخاب کرده و بقیه ی تنظیمات را بی تغییر نگه می داریم.
- یک نام مناسب تر برای Common name for this CA درج کرده و تا پایان پیش می رویم.

4. Certificate ایجاد می کنیم.

- باید یک Template برای احراز هویت SSTP VPN Server ایجاد کنیم و سپس یک Certificate از روی آن برای VPN Server ایجاد کرده و در سرویس RRAS قرار دهیم.
  - یا توسط Ctrl+M وارد کنسول MMC شده و آبجکت Certificate Template را از کادر سمت چپ Add می کنیم.
    آبجکت Certificates را برای Computer Account هم Add می کنیم.
    آبجکت Certification Authority را نیز Add می کنیم و OK!
    حال کنسول ایجاد شده را بر روی Desktop ذخیره می کنیم.
  - یا در Run درج می کنیم: certsrv.msc

روش اول:

- درون این کنسول وارد Certificate Templates شده و وارد Properties گزینه ی ..OCSP Response می شویم.
- در تب General گزینه ی Publish Certificate in AD و .Do not automatically reenroll را فعال می کنیم.
- در تب Security:
  خود این کامپیوتر را بصورت Full Contrl تعیین می کنیم.
  برای گروه های Domain Computers و Domain Contrllers،گزینه های Read، Eroll و Auto Enroll را می زنیم و OK!

- در همین کنسول و گزینه ی Cert.Tem ، از آبجکت IPSec یک Dublicate گرفته و در تب General یک نام مرتبط با VPN درج کرده (مثلاً VPN-Cert) و گزینه ی Publish Certificate in AD و .Do not automatically reenroll را فعال می کنیم.
- در تب Security:

- خود این کامپیوتر را بصورت Full Contrl تعیین می کنیم.
- برای گروه های Domain Computers و Domain Contrllers،گزینه های Read، Eroll و Auto Enroll را می زنیم.
- در تب Extensions گزینه ی Application Policies را زده و Edit و از طریق دکمه ی Add، گزینه های
- Client Authentication و Server Authentication را Add می کنیم.

- در تب Request Handling گزینه ی ..Allow Private Key.را فعال می کنیم و OK!

به جهت اینکه CA Server از طریق اینترنت قابل دسترسی باشد، باید یک آدرس به آن اختصاص دهیم که در اینترنت publish شود:

- در کادر سمت چپ، وارد آبجکت Certification Authority شده و بر روی آبجکت این سرور کلیک راست و Properties را زده و در تب Extensions برای گزینه ی Select Extnsns، گزینه ی AIA را می زنیم.
- در همین تب، Add را زده و در نوار Location آدرس سرور CA را (که در اینجا، همین سرور است) همراه با //:http وارد می کنیم.
- و OK . مثلاً: http://vpnserver.payamavar.local/ocsp
- در همان تب، گزینه ی ..include in the online certificate s را فعال می کنیم و Apply و OK!
- در کادر چپ کنسول، وارد آبجکت خود این سرور شده و بر روی پوشه ی Certificate Templates کلیک راست کرده و new و Certificate Template to issue را می زنیم.
- در کادر باز شده، گزینه ی OCSP Response Signing را زده و OK می کنیم.
- به همین طریق دوباره وارد شده و Certificate ای که خودمان ایجاد کردیم را وارد می کنیم (VPN-Cert).

روش دوم:

- بر روی Certificate Templates کلیک راست کرده و Manage را می زنیم.
- از آنجایی که قالب Certificate مربوط به SSTP و IPSEC خیلی مشابه هستند، می توان از Certificate آن کمک گرفت، پس بر روی IPSEC کلیک راست کرده و Duplicate Template را می زنیم:
- در تب Compatibility برای دو گزینه ی کرکره ای، باید حداقل ورژن ویندوزهای Server و Client موردنظر را انتخاب کنیم.
- در تب General یک نام برای این Template درج می کنیم. (در نوار display Name)
- در تب Request Handling، گزینه ی Allow Private key to be exported را فعال می کنیم.
- در تب Extensions می بینیم که در کادر پایین IP Security IKE وارد شده است، روی Edit زده و سپس روی Add می زنیم.
- گزینه ی Server Authentication را اضافه می کنیم.
- در تب Subject Name گزینه ی Supply in the Request را می زنیم.
- اگر یک هشدار داد، OK کرده و تمام!

در ادامه:

- دوباره بر روی Certificate Templates کلیک راست کرده و این بار، New و Certificate Template to issue را می زنیم.
- در پنجره ی باز شده، template ای که برای SSTP ایجاد کرده بودیم را اضافه می کنیم.

به جهت اینکه CA Server از طریق اینترنت قابل دسترسی باشد، باید یک آدرس به آن اختصاص دهیم که در اینترنت publish شود:

- در کادر سمت چپ، وارد آبجکت Certification Authority شده و بر روی آبجکت این سرور کلیک راست و Properties را زده و در تب Extensions برای گزینه ی Select Extnsns، گزینه ی CRL را انتخاب کرده و در کادر زیر آن، گزینه ای که با http شروع می شود را انتخاب کرده و Remove می کنیم و Add را می زنیم.
- در کادر توضیحات پایین، در خط Example location از ابتدای //:http را تا پایان کپی کرده و در نوار Location قرار می دهیم.
- سپس به جای <ServerDNSName> آدرس همین CA Server مان را درج می کنیم و بدون تغییر دیگری، OK می کنیم. مثلاً: vpnserver.payamavar.local
- حال در همان تب Extensions این گزینه ی اضافه شده را انتخاب کرده و همه ی گزینه های پایین این تب را فعال کرده و OK!

5. Certificate ایجاد شده را در Group Policy پیکربندی می کنیم.

از منوی Tools گزینه ی Group Policy Management را وارد می کنیم.

وارد Default Domain Policy شده و به مسیر زیر می رویم:

Computer Configuration > Policies > Windows Setting > Security Setting > Public Key Policies

گزینه ی Certificate Services Client – Auto Enrollment را باز می کنیم.

آن را Enabled کرده و گزینه های ...Renew expired Certificates, up و update certificates را فعال می کنیم.

و OK کرده و GP Management را بسته و در cmd درج می کنیم: gpupdate /force

6. کنسول Online Responder را پیکربندی می کنیم.

از منوی Tools وارد Online Responder Management می شویم.

در کادر سمت چپ و بالا، باید در زیرمجموعه ی Array Configuration، گزینه ی این سرور سبزرنگ باشد.

سپس بر روی Revocation Configuration کلیک راست کرده و Add Revocation Configu را می زنیم.

یک نام مرتبط با Server بودن برای Certification درج می کنیم (مثلاً: CertServer)

گزینه ی select a certificate for an Existing CA را می زنیم.

در تب Choose CA Certificate دکمه ی Browse را زده و Certificate ای که برای این سرور ساختیم را می زنیم.

در تب select Signing Certifcts باید گزینه ی Auto-Enroll فعال باشد و .OCSPResponseSi انتخاب شده باشد.

و finish!

7. برای VPN Server یک Certification را پیکربندی می کنیم.

روش اول:

- دوباره به تنظیمات Certification که در یک فایل MMC ذخیره کرده بودیم برگشته و در سمت چپ، در بالا، وارد
- گزینه ی Certificate Templates شده و وارد Properties مربوط به Certificate ای که خودمان ایجاد کردیم
- (VPN-Cert) می شویم.
- در تب Subject Name گزینه ی Supply in the request را انتخاب کرده و OK!
- حال وارد گزینه ی (Certificates (Local Computers و سپس پوشه ی Personal می شویم.
- بر روی پوشه ی Certificates کلیک راست کرده و All Tasks و Request New Certificate را می زنیم و Next!
- در تب Request Certificates گزینه ی Certificate ای که خودمان ساختیم را فعال کرده و وارد لینک آبی رنگ زیر آن شده و Type را بر روی Common Name قرار داده و برای Value طی سه بار Add کردن، نام FQDN و دو آدرس IP همین Server را درج می کنیم، یعنی 192.168.139.139 و 23.1.2.101 و vpnserver.payamavar.local.
- سپس Apply و OK کرده و در ادامه Enroll را زده و Finish!

روش دوم:

- وارد MMC شده و Add/Rmve Snap-in را زده و Certificates را Add کرده و Computer Account را انتخاب و OK می کنیم.
- وارد پوشه ی Personal شده و روی Certificates کلیک راست کرده و All Tasks و Request New Certificate را می زنیم و Next و صبر می کنیم تا Certificate های موجود را پیدا کند.
- Certificate ای که برای VPN ایجاد کرده بودیم را انتخاب می کنیم و روی هشدار زردرنگی که زیر آن قرار دارد کلیک کرده و در پنجره ی باز شده Type را روی Common name قرار داده و برای Value همان آدرسی که برای Publish این CA Server در اینترنت وارد کردیم را درج کرده و Add می کنیم و OK: vpnserver.payamavar.local
- Enroll را می زنیم.

در ادامه، باید تعیین کنیم که اگر کسی از محیط خارج، درخواست اتصال به پورت 80 را داشت، توسط NAT، به CA Server متصل شود.

- وارد RRAS شده و در زیرمجموعه ی IPv4 گزینه ی NAT را زده و در سمت راست، وارد Properties آبجکت آداپتور خارجی می شویم.
- در تب Services and Ports روی Web Server (HTTP) دوبار کلیک می کنیم.
- حال، اگر CA Server در یک سیستم دیگر است، برای Private Address آدرس آن را درج می کنیم و اگر CA Server هم در VPN Server است، درج می کنیم: 127.0.0.1

8. VPN Connection را در سیستم Client ایجاد می کنیم.

- در User2 وارد Open Network and Internet Setting و سپس بخش VPN می شویم.
- Add a VPN Connection را می زنیم.
- Provider آن Windows (built-in) خواهد بود.
- یک نام انتخاب می کنیم.
- برای Server Name or Add آدرس خارجی VPN Server را وارد می کنیم: 23.1.2.101
- VPN Type را برروی SSTP قرار داده و Type of Sign-in info را بر روی Certificate قرار داده و SAVE!
- حال برای اتصال که نیاز به User و پسورد دارد، برای User می توانیم VPN User ای که ایجاد کردیم را بصورت FQDN وارد کنیم.
- اگر سعی کنیم که این اتصال VPN را متصل کنیم، نمی شود؛ چون وقتی Certificate را چک می کند، چیزی پیدا نمی کند.

9. Public Key (CA Certificate) مربوط به CA Server را در سیستم Client نصب کنیم.

- با حساب VPN معمولی که از قبل داشتیم، در User2 به شبکه ی داخلی متصل می شویم.
- یک Browser را باز کرده و آدرس CA Server به صورت زیر وارد می کنیم:

http://192.168.139.139/certsrv

- اگر نیاز به Credentials باشد، مشخصات Admin را وارد می کنیم.
- در صفحه ی باز شده، روی Download a CA Certificate, Certificate chain, or CRL زده و در بالا، گزینه ی
- install this CA certificate را می زنیم و به محل دانلود آن فایل می رویم.

در حقیقت باید یکبار آن را برای Machine و یکبار برای Account نصب کنیم.

- فایل را وارد و Open کرده و install Certificate را می زنیم.
- Local Machine را انتخاب می کنیم.
- در تب Certificate Store گزینه ی ..Place all certificates in را زده و از Browse پوشه ی Trusted Root Certification A را انتخاب کرده و OK و Finish!
- و باید یک پیام نصب موفق دریافت کنیم و سپس این Certificate را ببندیم.

10. Certificate را در سیستم User2 اختصاص می دهیم.

- در همان سیستم User2 وارد MMC شده و Ctrl+M را زده و دوبار آبجکت Certificates را Add می کنیم:
- یکبار گزینه ی User account را انتخاب می کنیم و یکبار Computer account را؛ و OK!
- حال این کنسول MMC را نیز برای اطمینان، یکبار Save می کنیم.
- در کادر سمت چپ، وارد آبجکت Certificate – Current User می شویم.
- ابتدا نیاز به یک Certificate برای User مدیر این سیستم داریم.پس بر روی پوشه ی Personal کلیک راست کرده و
- All Tasks و سپس Request New Certificate را می زنیم.
- در تب Request Certificates گزینه ی User را انتخاب کرده و Enroll را می زنیم و Finish.
- در حقیقت در اینجا به حساب Administrator این Client یک گواهینامه اعطا کردیم.

- حال اگر به Certificate دیگر که برای Local Computer بود برویم، باید ببینیم که در آنجا هم اختصاص داده شده است؛ در غیراینصورت همین کار را برای این Certificate هم انجام می دهیم، فقط به جای User، گزینه ی Computer را می زنیم.
- این کنسول را دوباره Save کرده و می بندیم و VPN متصل شده را نیز قطع می کنیم.

11. Certificate را در VPN Server انتخاب می کنیم.

- در سیستم VPN Server وارد کنسول Routing and Remote Access می شویم.
- وارد Properties آبجکت مربوط به این Server می شویم.
- ابتدا اگر بخواهیم با IPv6 هم کار کند، باید در تب IPv6، نوار Subnet prefix را بطور صحیح پر کنیم.
- در تب Security وارد Authentication Methods شده و به جز unauthenticated access، همگی را تیک می زنیم.
- در پایین و قسمت SSL Certificate Binding برای گزینه ی Certificate گزینه ی Certificate ای که به نام همین Server ایجاد کردیم را انتخاب و Apply و OK می کنیم.

نکته1: اگر نمی دانیم کدام Certificate صحیح است، باید فایل MMC ای که در همین VPN Server (روش اول) ذخیره کرده بودیم را باز کرده و به Certificates – Local Com رفته و در پوشه ی Personal و Certificates دقت می کنیم که برای کدام گزینه ها، مقدار ستون Certificate Template به نام Certificate ای است که برای VPN ایجاد کرده بودیم (VPN-Cert) پس در آن تب Security ، باید نام این Certificate را انتخاب کنیم.
نکته2: احتمالاً دو گزینه برای این Certificate وجود دارد، پس فرق نمی کند که کدام را انتخاب کنیم.
و تمام! حال می توانیم در User2 ارتباط SSTP VPN را متصل کنیم.

اگر وصل نشد و خطایی در مورد CN Name داد، مثل:
CN name does not match the passed value
دوباره باید در سیستم VPN Server وارد کنسول Routing and Remote Access و Properties آبجکت مربوط به آن سرور و تب Security شده و مقدار گزینه ی Certificate را تغییر داد.
نکته: اگر در همین تب Security گزینه ی Authentication Provider را بر روی Radius و یا هرگزینه ی دیگر قرار دهیم، احتمالاً یک خطا می دهد، که تا آن را تنظیم نکنید، ارتباط VPN دیگر وصل نمی شود.
اما اگر دوباره آن را به گزینه ی Windows Authentication بازگردانیم، باید حتماً یکبار بر روی آبجکت این سرور در همین کنسول، کلیک راست کرده و All Tasks و Restart را بزنیم.

12. تنظیمات اختیاری را وارد می کنیم.

- می توانیم در Properties آداپتور SSTP VPN، در تب Security برای Data Encryption گزینه ی
- Maximum strength encryption را انتخاب کنیم تا رمزنگاری را با بالاترین شدت انجام دهد.
- در همین تب، وارد دکمه ی Properties زیر ..Use Extensible Auth.شده و گزینه ی .Use a certificate on.را زده و
- گزینه ی Connect to these Servers ر ا غیرفعال کرده و در کادر پایین، گزینه ای که به نام Certificate ایجاد شده برای سرور VPN می باشد را فعال می کنیم.(مثلاً: Payamavar-VPNSERVER-CA)

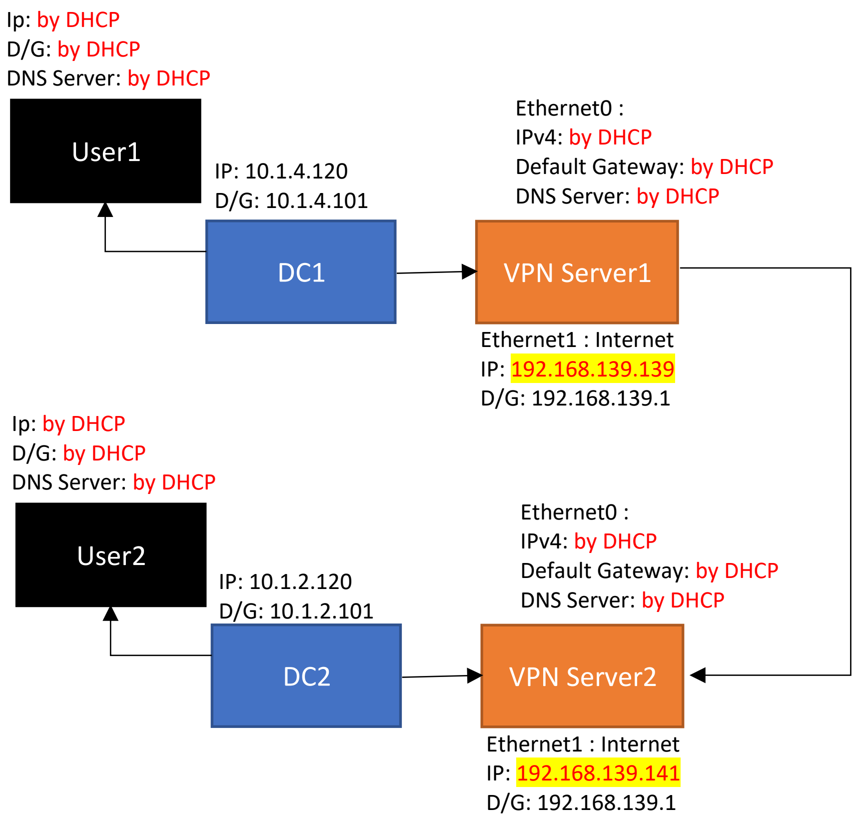
اگر بخواهیم برای اتصال، نیاز به User و Password باشد، باید در تب Security، گزینه ی کرکره ای مربوط به ..Use Extensible Auth.را روی (...Microsoft: Secured password (EAP-M قرار دهیم، و در این صورت نیاز به وارد کردن User و Password ای از سرور خواهیم داشت.

- در تب Networking می توان تیک IPv6 را فعال/غیرفعال کرد.

:IKEv2 VPN

برای راه اندازی این نوع **VPN Connection**، کافی ست ابتدا یک **SSTP Connection** ایجاد کنیم، سپس در سیستم **Client**، وارد **Properties** مربوط به **SSTP VPN Connection** ای که ایجاد کرده بودیم شده و در تب **Security** مقدار **Type of VPN** را روی **IKEv2** قرار می دهیم و دوباره متصل می شویم.

:S2S VPN (Site-to-Site) Implementation



در حقیقت در مثال واقعی، IP مربوط به Ethernet1 های هریک از VPN Server ها باید Public Static IP باشند.
درنتیجه باید بدون نیاز به اتصال VPN بتوان در هریک از VPN Server ها، به دیگری Ping کرد.
و از طرف دیگر، در محیط تست، نیازی به سیستم های User1 و User2 نمی باشد، نتیجه ی قابل قبول در DC ها کافیست.

1. در هریک از VPN Server ها، دو User جهت ایجاد تونل تعریف می کنیم.
   - پس در هریک از VPN Server ها به بخش User and Computers رفته و دو User همنام با server ها ایجاد می کنیم.
   - مثلاً به نام های VPNuser1 و VPNuser2
   - حال باید قابلیت Dial-In را برای آنها فعال کنیم، پس وارد Properties هریک از آنها شده و در تب Dial-In در قسمت Network Access Permission گزینه ی Allow Access را انتخاب می کنیم.

2. VPN را بر روی هردو VPN Server راه اندازی می کنیم. مثلاً برای VPN Server1
نکته: اگر نقش Remote Access به دلایل دیگر، از قبل روی این Server نصب بوده، بهتر است حذف و از نو نصب شود!
   - وارد کنسول Routing and Remote Access می شویم.
   - اگر در کادر سمت چپ این کنسول، آبجکت این Server موجود نبود، بر روی Routing and Remote Access کلیک راست و Add Server و سپس the Following Computer را زده و نام FQDN این سرور را درج و OK می کنیم.
   - بر روی Server اضافه شده، کلیک راست کرده و .Configure and enable Rout را می زنیم.
     - یا گزینه ی Custom Configuration را انتخاب کرده و سپس VPN access و Demand dial و NAT را فعال کرده و تمام!

     بر روی آبجکت NAT کلیک راست کرده و New Interface را زده و آداپتور خارجی را انتخاب و OK می کنیم.
     در پنجره ی باز شده، در تب NAT، گزینه ی Public و Enable NAT on this Interface را فعال می کنیم و OK!

- و یا گزینه ی Secure Connection between 2 Private Networks را انتخاب می کنیم.

Yes را انتخاب می کنیم.

در تب IP Address Assignment، باید تعیین کنیم که کاربرهایی که به VPN Server مان متصل می شوند، به چه شکل IP دریافت کنند. اگر Automatically را انتخاب کنیم، از DHCP Server شبکه داخلی مان آدرس دریافت می کنند، و اگر From a specified range را بزنیم، در تب بعد، باید یک محدوده از IP Address ها را درج و تعریف کنیم که از آنها، آدرس تخصیص بدهد؛ و Finish!

3. VPN را بر روی هردو VPN Server پیکربندی می کنیم.

- یک Wizard جدید باز می شود که یک Interface مجازی جهت ایجاد تونل با شبکه ی مقصد، ایجاد می کند.
  - اگر Wizard باز نشد، در همان کنسول RRAS، در آبجکت های زیرمجموعه ی Server، بر روی آبجکت Network Interfaces کلیک راست کرده و New Demand-dial Interface را می زنیم.
- برای نام آن، نام User ایجاد شده ی برای VPN Server مقصد را درج می کنیم: VPNuser2
- Connection Type را از نوع VPN قرار می دهیم.
- VPN Type را از نوع Automatic قرار می دهیم، البته می توان PPTP را هم انتخاب کرد.
- برای Destination Address آدرس IP و یا FQDN مربوط به VPN Server مقصد را درج می کنیم.
- برای Protocols and Security گزینه ی Route IP Packets on.. و Add a user account ... را فعال می کنیم.
- برای Static Route for Remote Networks یک Static Route تعریف می کنیم، یا می توان فعلاً Next را زد! و یا روی Add کلیک کرده و آدرس Network ID شبکه ی مقصد را همراه با Subnet Address آن درج و OK می کنیم.
- در Dial-out Credentials یک User ایجاد می کنیم.
- (همنام با User ای که برای همین Server ایجاد کردیم: VPNuser1)

- ➢ اگر در آن ویزارد، Static Route تعریف نکردیم، وارد آبجکت Server و گزینه ی IPv4 شده و بر روی Static Route کلیک راست و New Static Route را می زنیم.
- ➢ برای Interface، اینترفیسی که به نام User ایجاد شده، تعریف کردیم را انتخاب می کنیم.(VPNuser2)
- ➢ برای Destination، آدرس Network ID شبکه ی مقصد را درج می کنیم: یا 10.1.2.0 و یا 10.1.4.0
- ➢ برای Network Mask ، طبق مثال، آدرس 255.255.255.0 را درج کرده و تمام!

4. نوع ارتباط را برای هردو VPN Server تنظیم می کنیم.

- در کنسول Routing and Remote Access از زیرمجموعه ی آبجکت سرور، وارد Network Interfaces می شویم.
- وارد Properties گزینه ی Interface ای که ایجاد کردیم (VPNuser2) می شویم.
- در تب Options می توانیم نوع ارتباط را بر روی یکی از گزینه های زیر قرار دهیم:
- Demand-dial : زمانی که تونل به اندازه ی زمان تعیین شده، بی استفاده باشد، قطع شده و موقع نیاز، وصل می شود.
- Persistent : ارتباط بدون هیچگونه قطعی، همواره متصل است.

نکته: به جهت امنیت، گزینه ی Demand dial بهتر است!

- در تب Security می توانیم برای Authentication گزینه ی .Use Extensible Authe را انتخاب و از منوی زیر آن، گزینه ی Microsoft: Secured Password (EAP-MSCHAP v2...) را انتخاب کنیم.
- در تب Networking می توانیم گزینه ی IPv6 را غیرفعال کنیم.
- حال VPN Server را یکبار Restart می کنیم.

5. اتصال و ارتباط VPN بین هردو Site را تست می کنیم.

- **حال اگر در کنسول Routing and Remote Access در هریک از VPN Server ها به آبجکت Network Interfaces برویم، باید برای تب های Status و Connection State هریک از Interface هایی که ایجاد کردیم، Enabled و Connected درج شده باشد.**
- **اگر اینگونه نبود، بر روی Interface ایجاد شده، کلیک راست کرده و Connect را می زنیم.**
- **حال کافی ست از هریک از Server ها و هریک از Client های هردو شبکه، به شبکه ی دیگر Ping کنیم تا از برقراری اتصال مطمئن شویم.**

: NPS (Network Policy Server) working

1. بطور مثال یک VPN Server راه اندازی می کنیم.

2. Network Policy Server را پیکربندی می کنیم.

- در حقیقت این سرویس با نصب RRAS در Server، بطور سبک، نصب می شود و می توان از منوی Tools آن را باز کرد.

در کادر سمت چپ این کنسول:

- در گزینه ی Policies ، درون پوشه ی Connection Request Policies، سیاست هایی را می بینیم که در زمان درخواست یک Connection، ابتدا این Policiy ها بررسی می شوند، و اگر برقرار باشند، سپس به پوشه ی Network Policies می رود و سیاست های آنها را نیز بررسی می کند.

برای اتصال VPN Connection ها:

- ابتدا باید Policy های تعریف شده در پوشه ی Connection Request Policies بررسی و قبول شوند.
- سپس باید Policy های تعریف شده در پوشه ی Network Policies بررسی و قبول شوند.
- در خود این پوشه، به این شکل عمل می شود که:
- اگر درخواست اتصال به Server، با اولین Policy هماهنگ نبود، به Policy بعدی می رود و همینطور تا آخرین!
- اما اگر با یکی از Policy ها هماهنگی داشت، دیگر به Policy بعدی نمی رود.
- در درون هریک از Policy ها به این شکل عمل می کند که ابتدا درخواست، باید با Condition ها همخوانی داشته باشد، و اگر Condition ها را برآورده ساخت، سپس به تب Constraint های آن Policy می رود، و اگر همه ی محدودیت های تب Constraint را برآورده نکرد، از این Policy عبور می کند.
- اگر درخواست وارد شده، از همه ی Policy ها عبور کند، در پایان پاسخ آن را منفی می دهد!
  و سپس تازه به مرحله ی Authentication می رود.
- هریک از آبجکت های تعریف شده در پوشه ی Policy ها، قابلیت Dublicate شدن دارند که پس از duplicate شدن باید در تب Overview شان فعال نیز شوند.
- هر Policy ای که در خط بالاتر قرار داشته باشد، زودتر چک می شود.
- برای ایجاد برخی شرایط و Policy ها، وارد پوشه ی Connection Request P و تب Condition می شویم:
- برای تعیین اینکه یک VPN Connection در چه روزها و بازه های زمانی بتواند متصل شود، بر روی آبجکت Day and Time restrictions دابل کلیک می کنیم.
- برای تعیین اینکه یک VPN Connection با چه نوع tunneling Protocol ای بتواند متصل شود، بر روی Add کلیک و گزینه ی Tunnel Type را باز کرده و انتخاب می کنیم.
- و ...

- اگر بخواهیم تمام User هایی که Remote Client ها در VPN Connection شان برای اتصال به VPN Server استفاده می کنند را تحت کنترل داشته باشیم:
- در Domain Controller یک Group ایجاد کرده و همه ی User های مربوط به Remote Client ها را درون آن عضو می کنیم.
- در VPN Server به کنسول NPS و مسیر Policies > Network Policies رفته و یک آبجکت جدید ایجاد و فعال می کنیم.
- در تب Conditions گزینه ی Add را می زنیم.
- گزینه ی User Groups را Add کرده و سپس Add Groups را زده و Group ایجاد شده در AD را انتخاب و OK می کنیم.
- بقیه ی آبجکت های پوشه ی Network Policy را غیرفعال کرده و تست می کنیم.

- حال فرض کنید برای همه ی آبجکت های درون پوشه ی Network Policies گزینه ی Deny Access را انتخاب کنیم.با اینکه همچنان VPN User موردنظر عضو گروه ایجاد شده است، و این گروه هم در تب Conditions عضو شده است، همچنان اگر Client تلاش به اتصال به VPN Server کند، وصل نخواهد شد!

- حال از جهتی، می توان از قدرت AD DS کمک گرفت!
- پس به تنظیمات Properties حساب کاربری ای که برای آن Client در نظر گرفته شده است می رویم و در تب Dial-in، برای گزینه ی Network Access Permission، گزینه ی Allow Access را انتخاب می کنیم، تا این VPN Client User بتواند بی توجه به Deny/Allow Access در آبجکت NPS، متصل شود.

- اما اگر برای ما ضروری باشد که تمام User هایی که در آبجکت NPS وارد کرده ایم، بدون توجه به اینکه در تب Dial-in آن User ها چه چیزی تنظیم شده است، متصل شوند یا نشوند و نظر نهایی با خود NPS باشد، باید وارد Properties آبجکت موجود در Network Policies شده و در زیر گزینه های Grant/Deny access ، گزینه ی Ignore user account dial-in properties را فعال کنیم.

Radius :

(Remote Authentication Dial-in User Service)

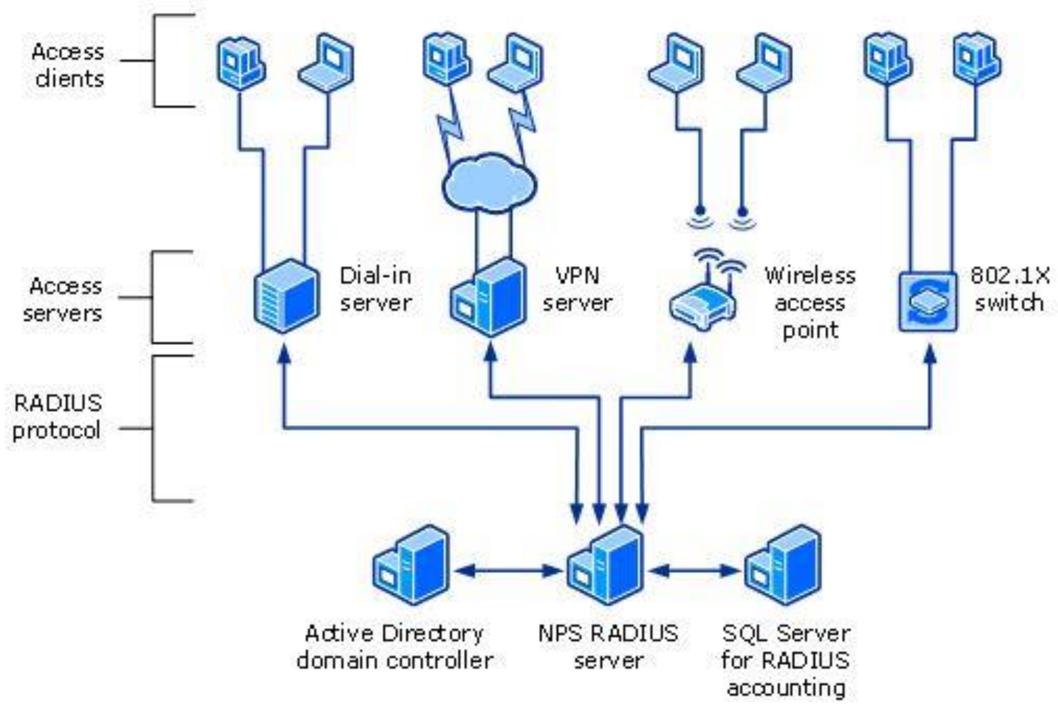
در حقیقت با **GPO** می توان برای **User** ها و **Client** های عضو شبکه، **Policy** تعریف کرد.
اما برای **User** هایی که از هرطریقی (**wired or Wireless**) و با هر سیستمی به شبکه متصل می شوند هم می توان **Policy** اعمال کرد و اجازه نخواهیم داد تا هر **User** ای با هر سیستم دلخواهی، به شبکه متصل شود.
از طرف دیگر اگر برخی **Client** های شبکه، از طریق **Remote Connection** ای مثل **VPN** یا **Dial-in** وصل شده باشند، نیاز خیلی واجبی به یک سیستم امنیتی قوی برای کنترل دسترسی ها و ورود و خروج ها خواهند داشت.
به همین منظور یک سیستم راه اندازی می کنیم به نام **RADIUS** !

- در زمینه ی **Radius** منظور از **Client**، یک **Client** با **User** معمولی نیست، بلکه منظور **Network Access Server** (**NAS**) هایی مانند **Dial-up server** ، **VPN server**، **Wireless access point** و یا **Proxy Server** است که هریک خودشان چندین **Client** معمولی را کنترل می کنند.
- پس به این اعضای متصل شده به شبکه، **Access Server** و به **Client** های معمولی آنها، **Access Client** گفته می شود.

به همین جهت، می توان از سرویس **Radius** (**Remote Authentication Dial-in User Service**) استفاده کرد که تحت کنسول **NPS** قابل بکارگیری است.

چه زمانی از Radius Server استفاده می کنیم؟

- زمانی که افراد توسط چندین **Access Server** به شبکه وصل می شوند.
- زمانی که قصد **authenticate** کاربرانی را داریم که عضو **Domain** نیستند و یا از اعضای با اعتماد دوطرفه نیستند.
- زمانی که تعداد درخواست ها زیاد است و بهتر است **load balancing** داشته باشیم.



همانطور که می بینیم، **Access Server** ها مثل **Client** برای **Radius Server** می شوند.

پس تا سرویس Radius تأیید نکند، هیچ ارتباطی از یکی از انواع زیر انجام نخواهد شد:

- Dial-Up Remote Access
- VPN Remote Access
- Wireless Access
- 1x Access
- Internet Access
- Extranet Access (دسترسی به شبکه ی سازمان شریک)

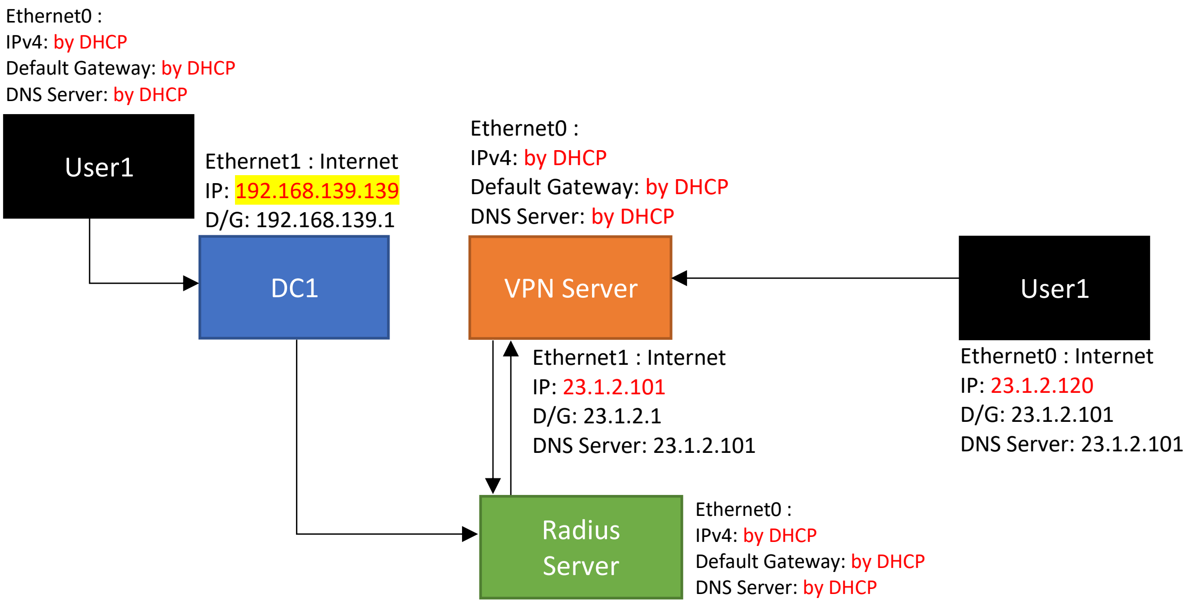
در حقیقت توسط Radius Server عملیات AAA (Authentication ، Authorization ، Accounting) را به صورت متمرکزتر انجام می دهیم.

در Radius Server :

- عمل Authentication به معنای این است که آیا User ای که قصد اتصال به شبکه را دارد، جزو User های ما در Active directory است یا خیر؟
- عمل Authorisation به این معناست که User ای که مرحله ی احراز هویت را پشت سر گذاشته است، به چه منابعی و تا چه سطحی دسترسی داشته باشد.
- عمل Accounting مشخص می کند که در چه زمان هایی این Client می تواند به چه میزان از منابع، دسترسی داشته باشد.

- ✓ Radius Server از احراز هویت 802.1x پشتیبانی می کند.
- ✓ Radius Server می تواند یک DC هم باشد.

: Radius Server Implementation



1. **ابتدا یک اتصال VPN را برای همه ی User های خارجی مثل User1، درون VPN Server تنظیم می کنیم.**
   - فرقی نمی کند که از نوع **Windows Connection** باشد یا **Connection Profile**.
2. **بر روی Radius Server نقش NPS را نصب می کنیم.**
   - برای نصب و راه اندازی و کار با این **Server**، نیاز به یک **User** با دسترسی کاملاً مدیریتی خواهیم داشت.
   - وارد **Add Roles and Features** وارد می شویم.
   - گزینه ی **Network Policy and Access Services** را انتخاب کرده و تا پایان پیش می رویم.
   - برای کار با کنسول آن، در **Tools** گزینه ی **Network Policy Server** را باز می کنیم.
3. **Policy مربوط به فعال سازی Radius را نصب می کنیم.**
   - برای اینکه **Radius Server** را راه اندازی کنیم، باید در درون کنسولِ **NPS**، یک **Policy** برای آن ایجاد کنیم.
   - در کادر چپ کنسول **Network Policy Server**، بالاترین گزینه یعنی **NPS (Local)** را انتخاب می کنیم.
   - فهرست کرکره ای را بر روی **Radius Server for dial-up…** قرار داده و روی گزینه ی **Configure VPN or Dial-up** کلیک می کنیم.
   - گزینه ی **VPN** را انتخاب کرده و یک اسم برای آن درج می کنیم.
   - در تب **Redius Clients** باید از طریق دکمه ی **Add** ، همه ی **Access Server** ها را انتخاب کنیم.
   - یک نام انتخاب و با دکمه ی **verify** سرور موردنظر را انتخاب می کنیم.
   - حال یک رمزعبور برای اتصال این سرور با **Access Server (VPN Server)** برای **Shared secret** تعیین می کنیم و **OK**!
   - در تب **configure Authentication Method**، گزینه ی **Extensible Authentication Protocol** را فعال کرده و برای نوار **Type** گزینه ی **Microsoft: Secured password – MSCHAPv2** را انتخاب می کنیم.
   - در تب **specify User Groups** باید گروههایی که اجازه ی دسترسی به این **Access Server** ها را دارند، انتخاب کنیم.
   - پس باید تمام **User** هایی که قرار است بتوانند از طریق این **VPN** متصل شوند را در سیستم **DC**، درون یک گروه قرار داد و آن گروه را در اینجا **Add** کرد.
   - در تب **specify IP Filters** می توانیم تعیین کنیم که به چه نوع آدرس هایی اجازه ی ورود بدهد و به چه نوع ندهد.
   - بسته به سیستم رمزنگاری موجود در سازمان، گزینه های **encryption** را فعال یا غیرفعال می کنیم.
   - فعلاً به **Realm name** نیازی نیست و **Finish**!
   - حال اگر به آبجکت **Policies** و سپس **Connection Request Policies** برویم، می بینیم که **Policy** ایجاد شده در کادر سمت راست قرار گرفته است که اگر در اولین جایگاه نبود، آن را **move up** می کنیم.
   - حال به پوشه ی **Network Policies** می رویم و اگر آبجکتِ **Policy** ایجاد شده در اولین جایگاه نبود، آن را **move up** می کنیم.

4. VPN Server را طوری تنظیم می کنیم که درخواست های Connection ای که به او می رسد را به Radius Server ارسال یا forward کند.

- پس در سیستم VPN Server، وارد کنسول Network Policy Server می شویم.
- در پوشه ی Policy واقع در کادر سمت چپ، وارد Connection Request P شده و وارد Properties مربوط به Microsoft Routiung and Remote Access.. شده و به تب Setting می رویم.
- در سمت چپ، Authentication را انتخاب کرده و در سمت راست، گزینه ی New را زده و در کادر جدید، یک نام تعیین کرده (مثلاً RDSGroup) و Add را می زنیم.
- در تب Address و در نوار Server باید آدرس IP یا FQDN مربوط به Radius Server را وارد کنیم.
- در تب Authentication / Accounting پورت های آنها را می بینیم که اگر در شبکه یا در میان Radius Server و VPN Server یک Firewall فعال باشد، باید این شماره پورت ها را باز کنیم.در همین تب، در نوار Shared secret همان پسوردی که در Radius Server وارد کرده بودیم را وارد می کنیم.
- برای اینکه همان پسورد برای Accounting هم باشد، تیک گزینه ی .. Use the same.را می زنیم.
- اگر در شبکه، بیش از یک Radius Server داشته باشیم، باید در تب Load balancing، یک اولویت و وزن برای هریک از آنها تعیین کنیم و OK!
- سپس در تب Setting که گزینه ی Authentication را انتخاب کرده بودیم، باید گزینه ی دوم یعنی
- .. Forward Requests to.را انتخاب در مقابلش، گروهی که ایجاد کردیم را انتخاب کنیم و Apply و OK!
- حال در پوشه ی Network Policies تمام آبجکت های ایجاد شده را disable می کنیم و تمام!

- حال کافی ست که در سیستم User1، یکبار اتصال VPN را برقرار کنیم که باید با موفقیت متصل شود.
- اگر بخواهیم این ارتباط را در Radius Server فوراً قطع کنیم، کافی ست در کنسول Network Policy Server و در پوشه ی Network Policies آبجکت ایجاد شده را Disable کنیم.

5. Accounting را تنظیم می کنیم.

- در VPN Server وارد کنسول NPS Server شده و در کادر سمت چپ، وارد Accounting می شویم.
- وارد گزینه ی Configure Accounting شده و تنظیم می کنیم که آیا درون یک File متنی و یا درون یک فایل SQL ذخیره شود.
- و یا اینکه می توان مکان دیگری درون یک Server دیگر در شبکه را برای ذخیره ی این گزارش گیری تعیین کرد.
- پس در همین کنسول NPS Server، وارد پوشه ی Connection Request Policies شده و به تب Setting رفته و Accounting را انتخاب و فعال کرده و یک سیستم را انتخاب می کنیم و OK!

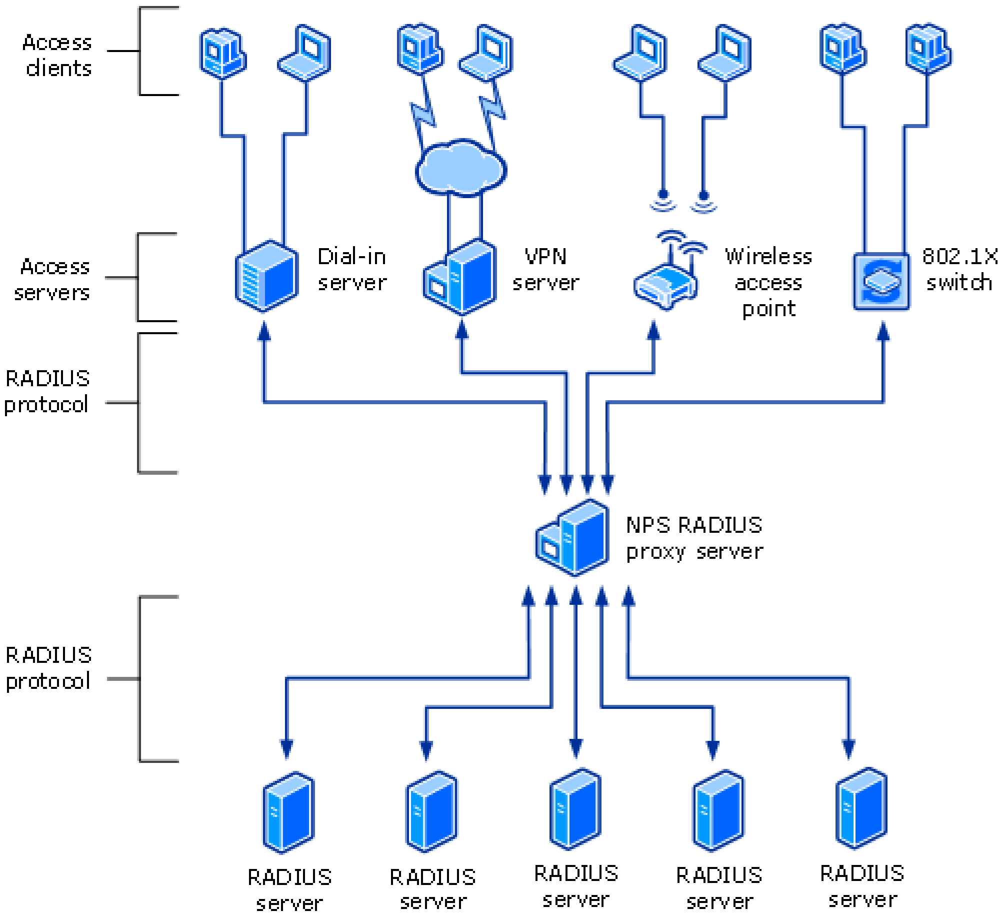
برای مشاهده ی آن Shared Secret می توان در PowerShell دستور زیر را نیز وارد کرد:

```
Get-NpsSharedSecretTemplate
```

: Radius Proxy Server

اگر به جهت زیاد شدن Access Server ها، نیاز به Radius Server های بیشتری داشته باشیم، در نتیجه کنترل اتصال ها و مدیریت ارتباط Access Server ها با Radius Server هم پیچیده خواهد شد!

پس می توانیم از یک Radius Proxy Server استفاده کنیم؛ به این صورت که تمام Access Server ها به یک سمت آن متصل شده و تمام Radius Server ها هم به سمت دیگر آن!



در حقیقت باید تمامی Access Server ها را به عنوان Client های Radius Proxy Server تعریف کنیم و خود Proxy Server را به عنوان Client برای Radius Server ها تعریف کنیم.

در حقیقت می توان برای رسیدگی به درخواست های هریک از Access Server ها، چندین Radius Server تعریف کرد، و آنها را در کنسول NPS، درون یک گروه قرار داد و اولویت بندی نیز کرد.

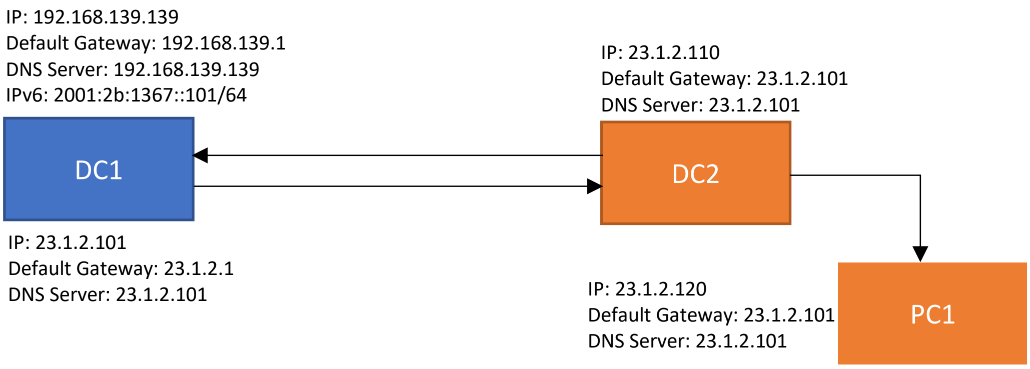
اما برای هریک از Access Server ها، نیاز به یک گروه جدید است.

1. در تک تک Radius Server ها، سرور Proxy را به عنوان Client تعریف می کنیم.
2. در تک تک Access Server ها، سرور Proxy را به عنوان Server بالادستی تعریف می کنیم.
3. در سرور Proxy، تمام Access Server ها را به عنوان Client تعریف می کنیم.
4. در سرور Proxy، تمام Radius Server ها را به عنوان Server بالادستی تعریف می کنیم.
5. در سرور Proxy، تعیین می کنیم که درخواست هریک از Access Server ها را به کدام Radius Server بفرستد.

ISATAP Connection :

ISATAP که مخفف Intra-Site Automatic Tunnel Addressing Protocol می باشد، روشی برای ایجاد ارتباط میان شبکه ای که با IPv6 کار می کند و شبکه ای که IPV4 کار می کند، در ویندوزهای Server است.
توسط این روش، می توان درون یک شبکه ی داخلی که با IPv6 کار می کند، یک تونل IPv4 ایجاد کرد و توسط آن با شبکه ای دیگر که با IPv4 کار می کند، ارتباط برقرار کرد.
در حقیقت در ویندوزهای غیر Server قابلیت ISATAP وجود ندارد؛ به همین دلیل وقتی بخواهیم یک سیستم که فقط با IPv4 کار می کند را عضو یک شبکه ی IPv6 کنیم، نیاز به یک سیستم Windows Server برای آن خواهیم داشت.

طبق شکل زیر، باید ISATAP Adapter را بر روی سرور DC1 فعال کنیم.
پس زمانی که DC2 قصد برقراری ارتباط با DC1 داشته باشد، با ISATAP Adapter آن ارتباط برقرار می کند.



1. کنسول RRAS را بر روی DC1 راسه اندازی می کنیم.

- در بخش Role Services، گزینه ی Routing را انتخاب می کنیم و تا پایان نصب پیش می رویم.
- از منوی Tools، وارد گزینه ی Routing and Remote Access می شویم.
- حال اگر در کادر سمت چپ این کنسول، آبجکت این Server موجود نبود، بر روی Routing and Remote Access کلیک راست و Add Server و سپس the Following Computer را زده و نام FQDN این سرور را درج و OK می کنیم.
- بر روی سرور اضافه شده، کلیک راست کرده و .Configure and enable Rout را می زنیم.
- گزینه ی Custom Configuration را انتخاب می کنیم.
- گزینه ی Lan Routing را انتخاب می کنیم و finish و Start Service را می زنیم.

2. قابلیت ISATAP را بر روی Interface مربوط به 23.1.2.101 پیکربندی می کنیم.

- در حقیقت بطور پیشفرض قابلیت ISATAP بر روی ویندوز Server فعال است.
- برای مشاهده ی آن، دستور زیر را وارد می کنیم، تا شماره ی InterfaceIndex آن را نیز بدست بیاوریم:

```
Get-NetIPInterface
```

- اگر چند گزینه برای ISATAP وجود داشت، می توانیم آداپتور NIC مربوط به 23.1.2.101 را یکبار خاموش کنیم و دوباره این دستور را بزنیم و ببینیم.
- اما اگر این قابلیت برای این Adapter فعال نبود، می توانیم آداپتور مربوط به 192.168.139.0 را خاموش کرده و دستور زیر را وارد کنیم:

```
Netsh interface isatap set state enabled
```

- دستور زیر را بافرض عدد 19 برای **ifIndex** برای **Ethernet1** ، وارد می کنیم:

```
Set-NetIPInterface -InterfaceIndex 19 -AddressFamily IPv6 -Forwarding Enabled -Advertising Enabled
```

- یک مسیر برای مقصدهای به آدرس **prefix-IPv6** شبکه ی داخلی، ایجاد می کنیم:

```
New-NetRoute -DestinationPrefix 2001:2b:1367::/64 -InterfaceIndex 19 -AddressFamily IPv6 -Publish Yes
```

- تعیین می کنیم که **isatap Interface** مربوط به آداپتور **23.1.2.101** باید آدرس های وارده را کپسوله کند:

```
Set-NetIsatapConfiguration -Router 23.1.2.101
```

3. تنظیمات ISATAP را بر روی PC1 پیکربندی می کنیم.

- وارد **PC1** شده و دو دستور زیر را به ترتیب وارد می کنیم، تا از فعال شدن قابلیت **ISATAP** در آن مطمئن شویم.
نکته: باید با قابلیت **Admin** وارد **PC1** شده باشیم.

```
Set-NetIsatapConfiguration -router 23.1.2.101
Get-NetIsatapConfiguration
```

قابلیت **IPv6** را در **PC1** غیرفعال می کنیم.

4. تنظیمات ISATAP را بر روی DC2 پیکربندی می کنیم.

- وارد **DC2** شده و دو دستور زیر را به ترتیب وارد می کنیم، تا از فعال شدن قابلیت **ISATAP** در آن مطمئن شویم.

```
Set-NetIsatapConfiguration -router 23.1.2.101
Get-NetIsatapConfiguration
```

- قابلیت **IPv6** را در **DC2** غیرفعال می کنیم.
- حال کافی ست دستور **ipconfig /all** را یکبار وارد کنیم تا ببینیم که یک آداپتور دیگر که دارای یک **IPv6** مطابق با شبکه ی داخلی مان می باشد را اضافه کرده است! که بخش **Interface suffix** این **IPv6** شامل **IPv4** همین **DC2** نیز می باشد.

5. ارتباط را تست می کنیم.

- وارد **DC1** شده و دستور زیر را وارد کرده و می بینیم که در بخش **Tunnel adapter isatap** مربوط به آداپتور **23.1.2.101** یک **IPv6** نیز در اینجا ایجاد شده است.

```
ipconfig /all
```

- این **IPv6** را کپی کرده و در سیستم **DC2** به آن **Ping** می کنیم که باید متصل شده و انجام شود.

Direct Access :

- Direct Access مزایای بسیاری نسبت به VPN دارد و جایگزین خوبی برای VPN است.
- با DirectAccess ارتباط کامپیوتر یک کاربر با مثلاً شبکه ی داخلی یک شرکت ساده و یکپارچه است.
- همچنین تا حد زیادی امن تر از VPN است.
- User ها دیگر نگران مشکلات متصل شدن به VPN و برقراری ارتباط مجدد در صورت قطعی نیستند.
- و البته نباید فراموش کرد که استفاده از VPN می تواند سرعت اینترنت را کاهش دهد.
- شاید Direct Access Implementation تا حدی دشوارتر از VPN باشد،اما ارزشش را دارد.
- این سرویس مبتنی بر IPv6 است که بر اساس Tunneling آدرس IPv4 کار می کند.

DA برخلاف VPN که باید بصورت دستی اجرا و تنظیم بشود، بصورت کاملاً خودکار اجرا و متصل می شود و نیاز به هیچ گونه نرم افزارخاصی ندارد. وقتی Client بیرون از سازمان باشد، تنها نیاز است که به اینترنت دسترسی داشته باشد، سپس بصورت خودکار ارتباط خود را بصورت امن با DA Server برقرار کرده و به شبکه متصل می شود.

- DA Server و DA Client تمام اطلاعات خود را با استفاده از IPv6 انتقال می دهند و از IPsec برای امن کردن ارتباطات و از AD Certificate، Kerberos و NTLM برای احراز هویت استفاده می کند.

- همچنین DA Client از WFAS (Windows Firewall with Advanced Security) و NRPT (Name Resolution Policy Table) استفاده می کند.

- در حقیقت DirectAccess توسط IPv6 کار می کند، در حالی که بیشتر Resource های عضو شبکه با IPv4 کار می کنند!
- DA برای حل این مشکل از Tunnel استفاده می کند.
- به این صورت که ترافیک IPv6 را در IPv4 کپسوله می کند و آن را منتقل می کند.
- در DA سه نوع Tunnel یا Transition Technology وجود دارد:
  - ✓ 6to4
  - ✓ Teredo
  - ✓ IP-HTTPS

Direct Access می تواند به سه صورت راه اندازی شود:

1. Perimeter و یا DMZ : با یک کارت شبکه و پشت firewall

باید پروتکل و Port های زیر بر روی Firewall باز باشد:

- IP Protocol ID 41 : در صورت استفاده از تونل 6to4
- UDP port 3544 : در صورت استفاده از تونل Teredo
- TCP port 443 : در صورت استفاده از تونل IP-HTTPS

2. Edge Server :

DA Server باید دارای دو NIC باشد که یکی External بوده و به محیط خارجی وصل است و دیگری Internal بوده و به شبکه ی داخلی یا همان Intranet وصل است که دارای یک Private IP است.

3. LAN :

فقط نیاز به یک کارت شبکه و IP Private دارد.

باید پروتکل و پورت های زیر بر روی Firewall باز باشند :

- TCP port 443
- Publish DirectAccess in firewall

❖ توصیه می شود که DA را پشت یک Firewall و در قسمت DMZ قرار دهید تا امنیت آن فراهم شود.

NLS (Network Location Server) :

شاید این سوال پیش بیاید که آیا وقتی کاربر درون سازمان است هم همچنان از DA برای اتصال به شبکه استفاده می کند یا نه! و اگر نه، پس در خارج از سازمان، وقتی لبتاپ را روشن می کنیم، چطور می داند که نیاز به DA دارد و به سادگی دوباره به شبکه وصل می شود؟!

NLS یک Website است که بر روی آن یک صفحه ی وب، میزبانی می شود.

DA Client قبل از اینکه ارتباط خود را با DA Server برقرار کند، اول بررسی می کند که داخل سازمان است یا خیر!
به این صورت که یک درخواست به سمت NLS ارسال می کند؛ اگر توانست با NLS ارتباط برقرار کند، یعنی هنوز داخل سازمان است و از DA استفاده نمی کند، درغیراین صورت متوجه می شود که بیرون از سازمان است، پس از DA استفاده می کند.
از طرف دیگر، این وب سایت NLS ، نیازمند یک SSL Certificate می باشد و همچنین یک DNS A Record !

DirectAccess Prerequirements :

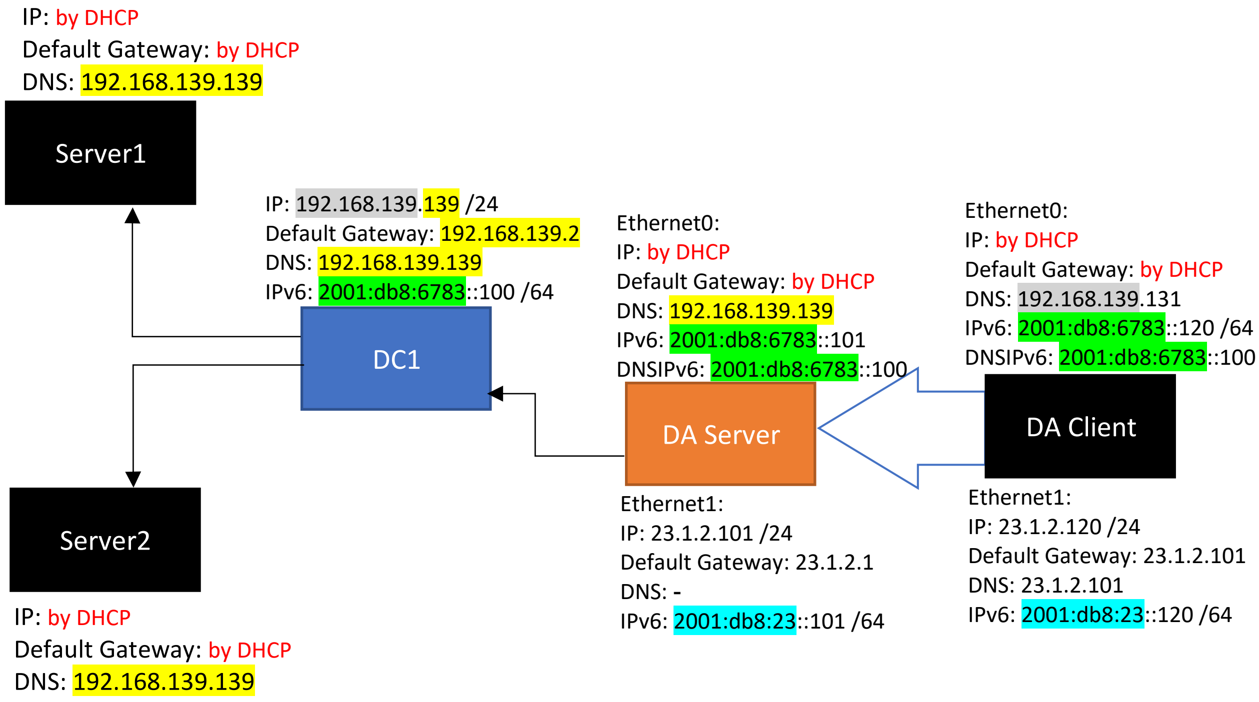
- DirectAccess از RODC پشتیبانی نمی کند و باید با یک Write Domain Controller ارتباط داشته باشد.
- Direct Access Server باید دارای سیستم عامل Windows Server 2008 R2 یا جدیدتر باشد.
- Direct Access Server باید دارای دو NIC که یکی به شبکه ی خارجی (اینترنت) و یکی به شبکه ی داخلی (Intranet) متصل است، باشد.
- DirectAccess Server باید Member Server باشد ولی به هیچ وجه Domain Controller نباشد، چون Error داده و صحیح نصب نمی شود.
- اگر DirectAccess را بر روی Hyper-V نصب می کنید، باید گزینه ی MAC address spoofing را بر روی آن VM فعال کنید.
- از نصب Firewall ها و آنتی ویروس های third-party بر روی DA خودداری کنید.

اگر به هر دلیلی مجبور به نصب چنین برنامه های شدید باید مطمئن شوید اینگونه برنامه ها مزاحم عملکرد DirectAccess نشوند و یا بعد از نصب موفقDA ، این برنامه ها را نصب کنید تا مراحل عیب یابی تا حدودی آسان شود.

- Windows Firewall باید بر روی DA Server و DA Client فعال باشد، چون IPsec در Security Rules Connection مربوط به Firewall ایجاد می شود.
- کاربری که مسئول نصب و Implementation DA می باشد، باید عضو Domain Admins باشد.

: DirectAccess Implementation

فرض کنید دارای یک اینچنین شبکه ای هستیم، که Direct Access Client یک کاربر در محیط خارج از Interanet است و می خواهد به شبکه متصل شود.



- در روش های نصب دیگر، بهتر است برای internal NIC مربوط به DA Server، هیچ default gateway تعریف نکنیم.
- برای external NIC مربوط به DA Server، هیچ DNS تعریف نمی کنیم.

1. در DC1 باید هم DHCPServer و هم DNSServer هم برای IPv4 و هم برای IPv6 فعال بوده و Dynamic Update آن فعال باشد.
   - قابلیت اختصاص دهی IPv6 را در DC1 برای آداپتور متصل به شبکه ی داخلی فعال می کنیم.
   - قابلیت اختصاص دهی IPv6 را در DA Server برای آداپتور Ethernet1 فعال می کنیم.
   - باید در DNS Server، مربوط به DC1، Forward Lookup Zone های Primary مربوط به IPv4 و IPv6 شبکه ی Intranet همراه با Reverse Lookup Zone های مربوط به آنها ایجاد شده باشند، و همه ی آنها در DNS Server مربوط به DA Server بصورت Secondary ایجاد شده باشند.
   - برای هیچ یک از Zone ها نباید DNSSEC فعال شده باشد.
   - پس باید وقتی در Direct Access Server هم به خودش و هم به DC1 دستور Nslookup را می زنیم، IPv6 های متناسب از DHCP دریافت کرده باشند.

2. به هر شکلی DA Client را عضو Intranet می کنیم که Default Group Policy مربوط به Intranet را دریافت کند.
   - ابتدا DA Client را کاملاً عضو Domain مربوط به شبکه ی داخلی می کنیم.
   - حال در حقیقت در این مثال، می توان به سادگی Ethernet0 مربوط به DA Client را Disable کرد و یکبار سیستم را
   - Shut down کرد تا از طریق Ethernet1 که فعال و به شبکه ی Intranet متصل است، این Client، Group Policy اش را به روز کند.

3. کنسول Direct Access را بر روی DA Server نصب و Implementation می کنیم.

- درست مثل RRAS Implementation، باید Role مربوط به Remote Access را نصب کنیم و پس از آن، در Server Manager و گزینه ی Tools، وارد کنسول Remote Access Management می شویم.
- در کادر سمت چپ و بالا، گزینه ی Direct Access and VPN را انتخاب کرده و سپس در کادر باز شده، گزینه ی
- Run the Getting Started Wizard را می زنیم.
- چون فقط می خواهیم Direct Access را نصب کنیم، پس گزینه ی وسط را می زنیم.
- چون DA Server را در میانه ی ارتباط با Client راه دور، قرار داده ایم، گزینه ی Edge را می زنیم.
- در کادر پایین، باید آدرس IPv4 آداپتوری که در DA Server به شبکه ی Public وصل می شود، یعنی Ethernet1 را درج کنیم.
- اگر Error ای به شکل زیر آمد، یا باید در Firewall یک Outbound Rule ایجاد کنیم که ارتباط بین خارج را با اعضای داخل شبکه ببندد و سپس یکبار Ethernet ها را قطع و وصل می کنیم؛ و یا از این سه گزینه، یکی دیگر را انتخاب کنیم:

An external adapter with a public IP address ipv6 enabled and without a domain profile Cannot be located.

- و next و finish!

- با توجه به اینکه از Getting Started Wizard برای پیکربندی DirectAccess استفاده کردیم، گزینه های زیر بصورت خودکار نصب و پیکربندی می شوند:
- تنظیمات DNS Host Record در Zone اصلی، شامل:

Directaccess-corpConnectivityHost
DirectAccess-NLS
Directaccess-WebProbeHost

4. Computer هایی که در راه دور قرار دارند را درون یک Group قرار می دهیم.

- در AD users and groups، یک Group جدید با نامی دلخواه، مثلاً DA، ایجاد کرده و کامپیوتر DA Client را درون آن عضو می کنیم.

5. GPO مربوط به Client ها را پیکربندی می کنیم.

- پس از نصب Direct Access در قسمت Step 1، بر روی دکمه ی Edit در زیر گزینه ی Remote Clients کلیک می کنیم.
- گزینه ی .Deploy full DirectAccess for Client access an را انتخاب می کنیم.
- آیکون Domain Computers را انتخاب و Remove می کنیم.
- دکمه ی Add را زده و گروه ساخته شده (DA) را وارد می کنیم؛ تیک .Enable Directaccess for mob را بر می داریم.
- در تب بعد، بر روی link درون کادر، کلیک راست کرده و Delete و دوباره راست کلیک کرده و new را می زنیم.
- در پنجره ی باز شده، منوی سمت چپ را بر روی Ping قرار داده و در جلوی آن، IPv6 مربوط به DC1 را درج و Add می کنیم.
- حال در نوار DirectAccess connection name، یک نام دلخواه برای این اتصال درج و تیک
- Allow DA Clients use local name را فعال کرده و Finish می کنیم.

6. GPO مربوط به DA Server را نیز پیکربندی می کنیم.

- در قسمت Step 2، بر روی دکمه ی Edit کلیک می کنیم.
- در نوار ظاهر شده، باید آدرس IP مربوط به Ethernet1 در DA Server را وارد می کنیم.(23.1.2.101)
- در تب Network Adapters در فهرست بالا، Ethernet1 (2001:db8:23::101) را انتخاب و گزینه ی ..Use a self-signed certificate cre را فعال نگه می داریم.
- در تب Prefix ها، باید Subnet prefix و عدد Prefix به درستی درج شده باشند، و اگر مثلاً 48 بود، باید آنرا 64 درج کنیم.
- اگر بخواهیم Client های با ویندوز 7 هم بتوانند متصل شوند، گزینه ی .Enable Win را فعال می کنیم و finish.
- پس فعلاً جهت ارتباط Direct Access، تا اینجا کافی ست، و در پایین سمت راست، finish را می زنیم.

- برای مشاهده ی صحت این اتصال، می توان در کادر سمت چپ، بالا، وارد گزینه ی **Dashboard** شد، و اگر گزینه یا گزینه هایی به رنگ زرد یا قرمز بودند، باید کادر سمت راست، بالا، **Refresh** را زده و چند دقیقه صبر کرد.
- پس دو **GPO** به نامهای **DirectAccess Client** و **DirectAccess Server** ایجاد کردیم که شامل موارد زیر هستند:
- تنظیمات **Certificate** ها و **IPsec** و **ICMP Protocol** و پروتکل **IP-http**
- تعریف پراکسی های **IPv6** و تنظیمات پروتکل **Kerberos** و ...

7. تنظیم بودن GPO را بر روی DA Server چک می کنیم.

- **PowerShell** را در **DA Server** باز کرده و درج می کنیم:

```
gpresult /r
```

- در زیر تیتر **Computer Setting** و زیرگزینه ی **Applied Group Policy Objects** باید گزینه ی DirectAccess Server Setting درج شده باشد.

8. تنظیم بودن GPO را بر روی DA Client چک می کنیم.

- **DA Client** را روشن می کنیم.(همچنان **Ethernet1** آن خاموش است.)
- در این سیستم **PowerShell** را باز کرده و درج می کنیم:

```
gpresult /r /scope:computer
```

- در زیر تیتر **Computer Setting** و زیرگزینه ی **Applied Group Policy Objects** باید گزینه ی **DirectAccess Client Setting** درج شده باشد؛ اگرنه؛ باید یکبار سیستم را **Restart** کنیم.

9. در DA Client اتصال را برقرار می کنیم.

- **Ethernet0** را فعال و **Ethernet1** را غیرفعال می کنیم.
- پس از چند دقیقه، اگر بر روی آیکون **Network** در سمت راست نوار **Task Bar**، کلیک کنیم، باید گزینه ی **Direct Access** مربوط به شبکه ی **Intranet** را ببینیم.
- اگر ظاهر نشد، یک بار سیستم را **Restart** می کنیم.

نکته:

برای حذف ابزار و کنسول Direct Access، در پنجره ی Remote Access Management و در کادر سمت راست بالا، بر روی گزینه ی Remove Configuration Settings کلیک می کنیم.

پس از آن، بهتر است که یکبار نقش Remote Access Service را حذف کنیم.

:(Quality of Service) QOS

در حقیقت در سازمان ها از QOS برای برطرف کردن نیازهای ترافیکیِ برنامه‌های حساس، مثل تماس‌های زنده ی صوتی یا تصویری استفاده می شود.

مثلاً اگر کارکنان از طریق شبکه، اقدام به ارسال فایل های حجیم برای یکدیگر کنند، و یا اینکه کارکنان برنامه هایی را از طریق Server و استفاده از اینترنت اجرا کنند، نباید خللی در استفاده ی آن‌ها از سیستم تلفن VOIP یا استفاده از تماس‌های تصویری با نرم‌افزارهای متداول تحت شبکه اتفاق بیافتد.

به کمک QoS از کاهش کیفیت ناشی از Packet Loss و Delay و ... جلوگیری می‌شود.

سازمان‌ها می‌توانند با استفاده از ابزار و تکنیک‌های خاصی نظیر تغییر میزان بافر و Traffic Shaping به نوعی QoS را اجرا کنند.

در بسیاری از سازمان‌ها بهره‌مندی از QoS در توافقنامه آن‌ها با سرویس دهنده ی شبکه، گنجانده شده است تا سطح مشخصی از کیفیت خدمات را تضمین کند.

سازمان‌ها می‌توانند QoS را از لحاظ کمّی، با استفاده از چند پارامتر، ازجمله موارد زیر اندازه‌گیری کنند:

- **Packet Loss** : از دست دادن بسته‌های داده زمانی اتفاق می‌افتد که پهنای باند لینک‌ها کاملاً اشغال‌شده باشند و روتر ها و سوییچ‌ها شروع به Drop کردن بسته‌ها نمایند.

  وقتی‌که در یک ارتباط زنده، مثل تماس‌های صوتی و تصویری Packet Loss اتفاق می افتد، باعث خلل در این تماس‌ها می شود.
- **Jitter** : نتیجه ی تراکم شبکه و تغییر مسیرهاست، که وقوع بیش‌ازحد آن می‌تواند باعث کاهش کیفیت ارتباط شود.
- **Latency** : منظور تأخیری است که طول می‌کشد تا یک بسته از مبدأ به مقصد برسد.این زمان باید تا حد ممکن به صفر نزدیک باشد.اگر در سیستم Voip این زمان زیاد باشد، می‌تواند موجب پژواک صدا و یا ایجاد همپوشانی شود.
- **Bandwidth** : پهنای باند یک لینک ارتباطی، میزان اطلاعاتی است که می‌تواند در یک بازه زمانی مشخص از نقطه‌ای به نقطه‌ی دیگر انتقال دهد. QoS با مدیریت پهنای باند و تنظیم اولویت برای برنامه‌ها، کیفیت ها را بهینه‌سازی می‌کند.
- **MOS** : یک معیار برای ارزیابی کیفیت صدا است که از یک مقیاس 5 گانه استفاده می‌کند.

- Modem ها یا Switch های مورد استفاده نیز باید قابلیت QoS را پشتیبانی کنند.
- از قابلیت های مودم های QoS، امکان کنترل و تعیین سرعت و حجم اینترنت برای هر کاربر (مثلا هرکدام از افراد خانواده) یا هر نرم افزار خاص می باشد.

Prerequirements to QoS Implementation :

چون QoS اقدام به کنترل Bandwidth نیز می کند، نیاز به راه اندازی یک Feature است که وظیفه ی اصلی اش اختصاص مقدار مشخصی از Bandwidth به هر نوع ترافیک است، می باشد، یعنی DCB (DataCenter Bridging).

- این باعث می شود که هرگاه برای یک نوع از ترافیک شبکه، مشکلی پیش آمده و ترافیک فوق سنگین شود، تاثیری روی ترافیک نوع دیگر نداشته باشد.
- اما دستگاه سروری که قصد دارد از سرویس DCB استفاده کند، باید دارای یک CNA باشد که DCB را پشتیبانی کند.

- CNA (Converged Network Adapter) یک Device است که هم دارای قابلیت های استاندارد شبکه های Ethernet است و هم دارای یک SAN HBA است.

✓ CNA ها درگاه های FCoE را نیز پشتیبانی می کنند.(Fiber Channel over Ethernet)

✓ شکل زیر نمایی از یک CNA می باشد:



- وقتی یک Server قرار است هم با شبکه LAN ارتباط داشته باشد و هم با SAN Storage، نیاز به دو کارت شبکه دارد.
  - یک Ethernet NIC جهت اتصال به شبکه ی LAN
  - یک SAN Host Bus Adapter که همان کارت HBA است، جهت اتصال به SAN Storage

نکته : سروری که دارای CNA هست، بجای اینکه یک Ethernet NIC و یک HBA داشته باشد، از فقط یک کارت CNA استفاده می کند.
نکته : از طرف دیگر Storage مورد استفاده نیز باید بتواند از قابلیت DCB پشتیبانی کند.

QOS Deployment :

وارد **PowerShell** می شویم:

1. **ابتدا Feature مربوط به DCB را نصب می کنیم.**

```
Install-WindowsFeature data-center-bridging
```

2. **شاید بخواهیم قابلیت DCB را از راه دور کنترل کنیم، پس این قابلیت را فعال می کنیم:**

```
Set-NetQosDcbxSetting -Willing $true
```

3. **قابلیت RDMA را برای Virtual Switch موردنظر فعال می کنیم.**

```
Enable-NetAdapterRdma "نام آداپتور"
```

4. **پورت SMB را در اولویت اول قرار می دهیم.**

از آنجایی که برای این سرویس، نیاز به پورت SMB (با شماره پورت 445) است، باید آن را در بالاترین اولویت قرار دهیم، پس طی تعریف یک Rule، تحت یک نام دلخواه (مثلاً smb) و شماره ی بالاترین اولویت (6) به آن اولویت اول را می دهیم:

```
New-NetQosPolicy "SMB" -NetDirectPortMatchCondition 445 -PriorityValue8021Action 6
```

5. **پورت های دیگر را در پایین ترین اولویت قرار می دهیم:**

```
New-NetQosPolicy "default" -Default -PriorityValue8021Action 1
```

6. **Class ترافیکی برای قابلیت QoS را تعریف می کنیم:**

```
New-NetQosTrafficClass "SMBClass" -Priority 6 -Algorithm ETS -BandwidthPercentage 30
```

7. **قابلیت DCB مربوط به کارت شبکه ی را فعال می کنیم:**

برای اینکه ببینیم کدام یک از NIC ها قابلیت QoS را پشتیبانی می کند، در PowerShell درج می کنیم:

```
Get-NetAdapterQos
```

حال برای فعال سازیِ آن، درج می کنیم:

```
Enable-NetAdapterQos -InterfaceAlias "نام آداپتور آن"
```

Web Application Proxy (WAP) Implementation:

اولین بار WAP در ویندوز سرور 2012 معرفی شد.

برای بکارگیری WAP به بستر AD FS نیازمند هستیم، چون Configuration آن در AD FS ذخیره می شود.

1. ابتدا باید رکورد DNS مربوط به Federation Service ای که ایجاد کردیم را در روی همان سیستم، تعریف کنیم.

- پس در کنسول DNS، روی نام DC در کادر سمت چپ کلیک راست کرده و New Host را می زنیم.
- برای Name، همان نامی که برای AD FS انتخاب کردیم را درج می کنیم.
- برای IP، آدرس خود سیستمی که روی آن AD FS را نصب کردیم، درج می کنیم.

نکته: نمی توان Web Application Proxy را بر روی همان سیستمی که Federation Service نصب کردیم، نصب کنیم؛ پس آن را روی یک سیستم دیگر نصب می کنیم.

- پس همان فایل Certificate که Export گرفتیم را به سیستم جدید برده و نصب می کنیم.
- Local Machine را زده و پسوردی که برای آن درج کرده بودیم را درج می کنیم.
- گزینه ی .. Automatically Select the Certificate Store based on را می زنیم و تمام!

2. برای نصب Web Application Proxy نیاز به راه اندازی نقش Remote Access خواهیم داشت.

- پس از طریق Add Roles and Features پیش می رویم و نقش Remote Access را انتخاب و چند قدم بعد، گزینه ی
- Web Application Proxy را انتخاب و Install می کنیم.
- پس از نصب، باید آن را Configure کنیم.
- برای Federation Service Name، نام دومینیِ سرویس Federation که در سرور آن تعیین کردیم را وارد می کنیم، مثلاً: fs.payamavar.local

- برای Username و Password، مشخصات یک local User Administrator را وارد می کنیم و نه یک Domain User.
- حال Certificate ای که نصب کردیم را انتخاب می کنیم.
- حال باید یک AD RMS را راه اندازی کنیم.

Active Directory Rights Management Services :

این سرویس، قوی ترین سرویس برای حفظ امنیت فایل هایی ست که توسط نرم افزارهای مختلف مثل Microsoft Office و Adobe Reader ایجاد شده اند.

- RMS از سیاست های IRM (Information Right Management) بهره می برد.
- با استفاده از این سیاست ها می توان Access Level مربوط به اسناد را تعیین کرد.
- مثلاً از اطلاعات در برابر پرینت گرفتن، کپی شدن و forward شدن توسط افراد غیر مجاز محافظت می شود.
- بزرگترین مزیت RMS این است که این سیاست ها به نوع فایل ها وابسته نیستند.
- این سیاست ها امکان منقضی شدن را نیز فراهم می کنند.
- اگر از SQL Server برای ذخیره ی Database مربوط به AD RMS استفاده شود، بهتر است.

نکته: قبل از نصب SQL Server هم ورژن به روز NET Framework. موردنیاز خواهد بود.

AD RMS Implementation :

1. یک User مخصوص ایجاد می کنیم و آن را عضو گروه های زیر می کنیم:
   - Domain Users
   - Domain Admins

2. Role آن را نصب می کنیم.

- به Add Roles and Features رفته و Role مربوط به Active Directory Right Management Services را انتخاب می کنیم.
- اگر AD FS را هم نصب داشته باشیم، برای Integrate شدن آنها با هم، Identity Federation Support را هم فعال می کنیم.
- پس از نصب، بر روی perform additional Configuration می زنیم.
- گزینه ی Create a new AD RMS را انتخاب می کنیم.
- باید مشخص کنیم که Database سیستم مان چه است، SQL Server و یا Data base خود سیستم.
- حال آن User ای ایجاد کرده بودیم را انتخاب می کنیم.
- نوع رمزنگاری را به دلخواه بر روی Mode 2 قرار می دهیم.
- . Use AD RMS Centrally managed را می زنیم.
- گزینه ی . Use an SSL Encrypted را زده و برای آدرس http، همان نام دومینیِ سرویس Federation را می نویسیم:

fs.payamavar.local

- در صفحه ی بعد، Certificate ای که نصب کردیم را انتخاب می کنیم، که نام PC صادر کننده ی Certificate همراه با آدرس Root DC می باشد.
- یک نام برای این سرویس RMS انتخاب و گزینه ی Register SCP Now را زده و سپس نام Federation Name را وارد کرده و نصب می کنیم.

fs.payamavar.local

Active Directory Lightweight Directory Services :

نرم افزارهایی که نیاز به Database شبکه دارند، توسط این سرویس در شبکه کنترل و مدیریت شده و اطلاعاتشان در آن ذخیره می شوند.

Windows Server Update Services (WSUS):

فرض کنید چندین سیستم Client و چندین سیستم با Windows Server در شبکه مان داشته باشیم.
وقتی تک تک آنها سعی در برقراری با سایت Microsoft داشته باشند تا update ها را دریافت کنند، اولاً حجم و فشار زیادی از تبادل داده بر روی خط اینترنت مان وارد می شود که منطقی نخواهد بود. دوماً مدیریت Update های Client ها و Server ها مختلف تحت کنترل کامل نخواهند بود.
پس یک Server را جهت دریافت Update ها از سایت Microsoft راه اندازی می کنیم و بقیه ی Server ها، update ها را از آن دریافت می کنند.
هر WSUS Server قادر به پشتیبانی 25 هزار سیستم جهت تامین Update های آنها خواهد بود.

پنج حالت برای راه اندازی WSUS وجود دارد:

- **Single WSUS Server :**

فقط یک سیستم به عنوان WSUS Server فعال خواهد بود که Update ها را دریافت و در شبکه پخش می کند.

- **Replica WSUS Server:**

در این حالت یک شرکت را با حداقل دو شعبه ی A و B در نظر بگیرید.
یک WSUS Server در شعبه ی A خواهیم داشت که update ها را مستقیم از Microsoft دریافت کرده و به اعضای شبکه در شعبه ی A می رساند.
در شعبه ی B هم یک WSUS Server خواهیم داشت که البته با Microsoft هیچ ارتباطی نخواهد داشت، بلکه Update ها را از WSUS Server شعبه ی A دریافت کرده و به Client های شعبه ی B می رساند.
درحقیقت در این روش، از طریق همان WSUS Server در شعبه ی A ، Update های Client های شعبه ی B را کنترل می کنیم.
پس به WSUS Server در شعبه ی B گفته می شود: <u>Replica WSUS Server</u>

- **Autonomous WSUS Server:**

اگر در همان مثال قبل، Update های مربوط به Client های شعبه ی B، توسط WSUS شعبه ی B مدیریت شوند، به Server B گفته می شود: <u>Autonomous WSUS Server</u>

- **Low Bandwidth WSUS Server:**

اگر در همان مثال قبل، WSUS شعبه ی B، تنها لیست جدیدترین Update ها را از WSUS Server شعبه ی A دریافت کرده و خودش تصمیم بگیرد که کدام را نیاز دارد، و آنها که موردنیازش است را خودش از Microsoft دریافت کند، به آن <u>Low bandwidth WSUS</u> گفته می شود.

- **Disconnected WSUS Server:**

اگر در همان مثال قبل، کلیه ی update های جدید، در WSUS Server شعبه ی A دریافت و بر روی یک دستگاه جانبی مثل Hard Disk ذخیره شده و به WSUS Server واقع در شعبه ی B برده شده و در آن import و ارایه شوند، به آن <u>Disconnected WSUS Server</u> گفته می شود.

Single WSUS Server Implementation :

در ابتدا روی سیستمی که جهت WSUS انتخاب کرده ایم، Windows Server را راه اندازی کرده و آن را عضو Domain می کنیم.

1. Role مربوط به WSUS را نصب می کنیم.

- وارد Add Roles and Features شده و در تب Roles، گزینه ی Windows Server Update Services را انتخاب کرده و در تب Role Services، گزینه های .WID Con و .WSUS Ser را انتخاب می کنیم.
- گزینه ی Store updates in the following location را فعال کرده و در نوار آن، یک آدرس جهت ذخیره سازی فایل های دانلود شده درج می کنیم. (مثلاً C:\update)
- ویزارد را بدون تغییر خاصی به پایان می رسانیم.
- به Server manager رفته و روی پرچم کوچک کنار Manage کلیک کرده و بر روی Launch Post-Installation tasks کلیک کرده و صبر می کنیم تا تمام شود.
- سپس در همان Server manager به بخش All Servers رفته و روی سرور WSUS کلیک راست کرده و Windows Server update Services را می زنیم.
- در کادر سمت چپ، بر روی Update Services کلیک راست کرده و Connect to Server را می زنیم.
- برای Server name آدرس FQDN خود WSUS Server را و برای Port number عدد 8530 را درج می کنیم و Connect.
- تیک گزینه ی ... Yes, I would like to join the را بر می داریم.
- در اینجا گزینه ی Synchronize from microsoft Update را می زنیم.
- گزینه ی Start Connecting را می زنیم تا یک سری اطلاعات مربوط به Update ها را دریافت کند.
- سپس ..Download updates only in را زده و فقط گزینه ی English را تیک می زنیم.
- در تب Products بسته به محصولات مورد استفاده در شبکه، گزینه ها را تیک می زنیم، مثلاً فقط Windows server 2016 و Windows 10 را.
- در تب Classifications فعلاً فقط گزینه های Critical updates و Security Updates را فعال می کنیم.
- Synchronize manually را انتخاب می کنیم. (خواه ناخواه، Update ها که بطورخودکار هم دانلود شده باشند، جهت نصب نیاز به تایید خود ما خواهند داشت.)
- .Initial Synchr را غیرفعال نگه داشته و Finish.

- ✓ سپس در کادر سمت چپِ کنسول می بینیم که Update Server اضافه شده است.
- ✓ اگر به زیرگزینه های آن و به آبجکت Options برویم، می بینیم که تمامی تنظیماتی که در طی نصب WSUS انجام دادیم را می توانیم در بخش های مجزا، دوباره تنظیم کنیم.
- ✓ برای دریافت جدیدترین Update از سایت Microsoft، کافی ست آبجکت خود WSUS Server را در بالای کادر چپ کنسول انتخاب کنیم، و در سمت راست کادر میانی، در بخش .Synch. Status روی گزینه ی Synchronize Now کلیک کنیم.

پس از پایان این همسان سازی، در کادر بالای آن (To Do) گزینه های دریافتی را لیست می کند که جهت نصب باید تایید شوند.

تهیه ی Update های جدید:

- برای مشاهده ی گزینه های Update دریافت شده به شکل جز به جز، به آبجکت All Updates رفته و در گزینه های بالای کادر میانی، Status را بر روی Any قرار می دهیم.
- برای اینکه update های قدیمی و جدید را بطور دو دسته ی پشت سر هم لیست کنیم، در نوار بالا روی Title کلیک راست کرده و Supersedence را می زنیم و سپس یکبار روی خود Title کلیک می کنیم.
- حال از نما و شکل آیکون Supersedence که پشت تک تک سطرهای این لیست قرار گرفته است، مشخص است که کدام یک قدیمی و احتمالاً نصب شده است و کدام یک جدید است.
- معمولاً آیکون Update های جدید، به شکل یک شمای سلسله مراتبی است که نقطه ی بالایی به شکل تیره تر است.
- پس همه ی گزینه های قدیمی را انتخاب و کلیک راست زده و Decline را می زنیم.
- حال به آبجکت Options رفته و در کادر روبرو گزینه ی Server Cleanup Wizard را می زنیم. همه گزینه ها را انتخاب کرده و Next کرده و finish.

کامپیوترها را گروه بندی می کنیم:

- کامپیوترهایی که قرار است به این Update Server متصل شوند، باید گروه بندی شوند.

پس از آبجکت های سمت چپ، به Computers رفته و بر روی All Computers کلیک راست کرده و Add Computer Group را می زنیم.

- یک نام برای آن انتخاب می کنیم. (مثلاً برای Server ها : Servers و برای PC ها: PCs)
- حال ممکن است دو دسته Server داشته باشیم، Server 2012 و 2016 ، پس دو زیر گروه هم برای آنها ایجاد می کنیم.

Computer ها را به Group هایی که ایجاد کردیم، اختصاص دهیم (assign کنیم):

این کار به دو شکل قابل انجام است:

- Server side Targeting: در این روش admin باید در خود کنسول WSUS سیستم ها را اضافه و وارد Group ها کند.
- Client side Targeting: این روش از طریق تنظیمات Group policy انجام شده و Client به طورخودکار خودشان را به WSUS Server معرفی می کنند.

در اینجا به روش <u>Client side targeting</u> عمل می کنیم:

- آبجکت Options را انتخاب کرده و وارد گزینه ی Computers می شویم.
- گزینه ی Use Group Policy را انتخاب می کنیم.
- حال کنسول AD Users and Computers را باز می کنیم.
- دقیقا همان Group بندی که در کنسول WSUS ایجاد کردیم را توسط OU ها ایجاد کرده و کامپیوترها و Server ها را درون OU های مربوط به خودشان جابجا می کنیم.
- به کنسول Group Policy Management می رویم.
- بر روی OU مربوط به Servers که کلیک راست کرده و ...Create a GPO in this را زده و یک نام برای آن درج کرده و آن را ایجاد کرده و وارد Edit آن می شویم.
- به مسیر زیر می رویم:

Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update

- در کادر روبرو، وارد تنظیمات Confgure Automatic Updates شده و Enable را انتخاب کرده و در پایین گزینه ی Automatic update را بر روی Auto download and schedule the install قرار می دهیم و OK.
- وارد تنظیمات Specify intranet Microsoft update service location شده و آن را enable کرده و برای هر دو گزینه ی اول در پایین، باید آدرس کامل WSUS Server را همراه با port آن درج کنیم و OK، به صورت زیر:

http://wsus.itpro.local:8530

- وارد تنظیمات Enable client-side targeting شده و آن را enable کرده و در نوار Target group در پایین، باید نام Group هایی که در کنسول WSUS ایجاد کردیم را درج کنیم، که میان نام آنها یک semicolon نیاز است که درج کنیم و OK، مثلاً:

Servers;PCs

Computer ها را مجبور می کنیم (force می کنیم) که Group policy که تنظیم کردیم را (Server Updates) دریافت کنند:

- در خود سیستم Server ای که هستیم، دستور زیر را برای سیستم های موجود وارد می کنیم. مثلاً:

```
icm server1,server2,PC1,PC2 {gpupdate /force}
```

- حال برای اینکه نتیجه را چک کنیم که تاثیر این Group policy را مشاهده کنیم، کافی ست دستور زیر را وارد کنیم:

```
icm server1,server2,PC1,PC2 {gpresult /r}
```

- در نتیجه ی ظاهر شده، به قسمتی که Applied Group Policy Objects را نشان می دهد رفته و زیر خطِ آن را مشاهده می کنیم که باید نام Group Policy تنظیم شده، یعنی Server Updates درج شده باشد.
- حال نیاز است که چند دقیقه ای صبر کنیم و یا دستور زیر را در PowerShell وارد کنیم و سپس به کنسول WSUS رفته و Group هایی که ایجاد و تنظیم کردیم را چک کنیم، که باید Client ها و Server هایی که به آنها assign کردیم را مشاهده کنیم.

```
icm server1,server2,PC1,PC2 {wuauclt /detectnow}
```

نکته: اگر پس از مدتی، همچنان Client ها در این Group ها ظاهر نشدند، به PowerShell رفته و دستور را وارد می کنیم:

```
icm server1,server2,PC1,PC2 {Get-Service wuauserv | Stop-Service}
```

حال با دستور زیر، Service های WSUS را فراخوانی می کنیم که باید در حالت Stopped باشند.

```
icm server1,server2,PC1,PC2 {Get-Service wuauserv}
```

دوباره آنها را روشن می کنیم و دوباره سعی در پیدا کردن WSUS client ها می کنیم:

```
icm server1,server2,PC1,PC2 {Get-Service wuauserv | Start-Service}

icm server1,server2,PC1,PC2 {wuauclt /detectnow}
```

Update ها را نصب می کنیم و پایان:

در کنسول WSUS به آبجکت Updates و سپس به All Updates رفته و همه ی گزینه های Update موجود را انتخاب و کلیک راست کرده و Approve را می زنیم و در پنجره ی باز شده، برای هریک از گروه های سلسله مراتبی که ایجاد کردیم، روی آیکون پشت شان کلیک کرده و Approve for install را می زنیم که آماده ی نصب شوند، که البته طبق Schedule ای که تنظیم کردیم، شروع به نصب خواهند شد.

اما برای اینکه این approve کردن ها، بطور خودکار انجام پذیرند، به آبجکت Options رفته و وارد گزینه ی Automatic approvals شده و در تب Update Rules گزینه ی Default Automatic Approval Rule را فعال می کنیم و همچنین می توان گزینه ی New Rule را زده و برای شرایط خاص هم یک شرایط approve خاص خودش را تنظیم کرد.

جهت دریافت و انجام Update مربوط به Windows Defender:

به آبجکت Options رفته و وارد گزینه ی Product and Classifications شده و در تب Products، علاوه بر نسخه های ویندوز موردنیازی که انتخاب کرده بودیم، گزینه ی Windows Defender را نیز فعال می کنیم و OK.

که البته لازم است که یکبار دیگر، به آبجکت اصلی این کنسول، یعنی WSUS Server رفته و در سمت راست کادر میانی، یکبار گزینه ی Synchronize now را بزنیم.

: Proxy Server

بطورمثال، در حالت معمول، یک کامپیوتر عضو شبکه، هنگامی که درخواست دسترسی به یک Website را دارد، مستقیماً به آن متصل شده و آن را باز می کند.
اما وقتی که Proxy Server داشته باشیم، سیستم Proxy Server درخواست کامپیوتر Client را دریافت کرده و خودش درخواست دسترسی را به آن Website ارسال می کند و وقتی آن را دریافت کرد، آن را به Client بر می گرداند.

در حقیقت Proxy Server، سروری است که نقش واسطه را میان Client ها و Server های دیگر ایفا می کند.
پس وقتی یک Client بخواهد فایل یا اطلاعاتی را از یک Server خارج از شبکه ی خودش دریافت کند، درخواستش را به Proxy server متصل می شود.
Proxy Server، کاربرها را از دسترسی های خطرناک محافظت می کند و همچنین قابلیت گزارشگیری از ترافیک های درون و بیرون سازمانی را فراهم می کند.

: Access Control

می‌توان از Proxy Server برای بهبود عملکرد یک شبکه و یا Filtering نیز استفاده کرد.
مثلاً Proxy Server می‌تواند Inbound Traffic و Outbound Traffic شبکه را بررسی کند و به آنچه که با معیارهای امنیتی یا سیاست سازمان مغایرت دارد، اجازه عبور ندهد.
و یا می توان در Proxy Server دسترسی به برخی صفحات اینترنتی را برای Client های شبکه، مسدود کرد.

:Security

استفاده از Proxy Server امنیت شبکه را در برابر نفوذگرها بالا می برد. به این صورت که استفاده از فضای بیرون شبکه را به صورت کاملاً ناشناس و نامحسوس می کند.
طوری که هیچکس تشخیص نمی دهد که کدام Client داخلی، کدام صفحات و منابع اینترنتی را درخواست داده است.

: Speed and Bandwidth

با توجه به اینکه، وقتی یکی از Client ها یک وبسایت را درخواست می دهد، یک کپی از آن وبسایت، در حافظه ی Cache مربوط به Proxy Server ذخیره می شود، در صورتی که هریک از Client های دیگر شبکه، آن وبسایت را درخواست دهند، پاسخ آنها از سمت Cache خود Proxy Server ارسال خواهد شد که باعث افزایش سرعت دسترسی ها می شود.
و اینکه دیگر نیازی به درخواست دسترسی مستقیم به خود وبسایت در فضای اینترنت نیست، باعث صرفه جویی در استفاده از Bandwidth می شود.

: Activity Logging

توسط Proxy Server، می توان به سادگی گزارشی از تمام صفحات اینترنتی که هریک از Client ها درخواست کرده و مشاهده کرده اند را همراه با مدت زمانی که در آنها گذرانده شده است را تهیه کرد.

: VPN

یکی از معایب Proxy Server این است که داده ها و اطلاعات مبادله شده ی Client های شبکه در فضای اینترنت، هیچگونه رمزنگاری و محافظتی نمی شوند، در نتیجه توسط نفوذگرها و ... قابل مشاهده خواهند بود.
به همین جهت در Proxy Server می توانیم از قابلیت VPN هم استفاده کنیم.

FSRM (File Server Resource Manager) :

مدیریت منابع **File Server** که به آن **File Server Resource Manager** یا بطور اختصار **FSRM** گفته می شود، یکی از قابلیت های ویندوز **Server** می باشد.

این قابلیت شما را قادر می سازد تا بتوانید داده های ذخیره شده در **File Server** را طبقه بندی نموده و بهتر مدیریت کنید.

نکته : قابلیت **FSRM** تنها بر روی دیسک های با فرمت **NTFS** کار می کند.

FSRM شامل پنج خصوصیت زیر می باشد:

مدیریت سهمیه :

این خصوصیت به شما این امکان را می دهد تا یک میزان مشخص از فضا را برای پوشه یا حجم خود تعیین کنید، همچنین امکان ایجاد پوشه بطور خودکار در داخل حجم را نیز انجام می دهد.

زیرساخت طبقه بندی فایل :

یک امکان موثر در خصوص مدیریت دسته بندی و طبقه بندی فایل ها ارائه می دهد که در کنار آن می توان داده های خود را نیز تجزیه و تحلیل نمود. شما دسته بندی خود را انجام می دهید سپس به این دسته بندی **Policy** مورد نظر خود را اضافه می کنید.

مثلاً سطح دسترسی به یک فایل و یا تاریخ انقضای آن را تعریف می کنید.

وظایف مدیریتی فایل :

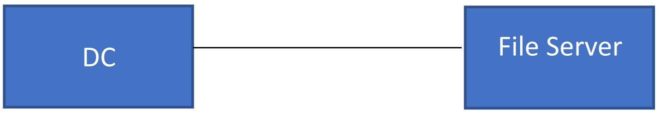
مدیریت غربالگری فایل :

با استفاده از این خصوصیت شما نوع فایل هایی که اجازه ذخیره سازی در **File Server** را دارند تعیین می کنید.

گزارش گیری از فضای ذخیره سازی :

این خصوصیت نحوه استفاده از دیسک و همچنین طبقه بندی اطلاعات و میزان فضای باقیمانده را نشان می دهد.

:Deploy the FSRM



می خواهیم FSRM را بر روی File Server راه اندازی کنیم.

1. FSRM را نصب می کنیم.

از طریق Add Roles and Features گزینه ی مربوط به نقش File and Storage Services را انتخاب کرده و از زیرگزینه های آن، File and iSCSI Services را باز و گزینه ی File Server Resource Manager را فعال کرده و نصب را تا پایان می رویم.

2. کنسول FSRM را باز می کنیم.

از طریق Server Manager و منوی Tools به سادگی کنسول File Server Resource Manager را باز می کنیم.
در کادر چپ، چند آبجکت مدیریتی وجود دارد.

3. Quota Management :

فرض کنید در سیستم File Server، دارای Drive D هستیم که دارای حجم 150 GB می باشد.
اگر یک پوشه در این درایو ایجاد کنیم و به اشتراک بگذاریم.
حال آن User هایی که می توانند این پوشه را ببینند، می توانند از آن یک Map Drive ایجاد کرده و درون آن مبادلات فایل و داده انجام دهند.
درحقیقت حجم قابل استفاده از این پوشه که تبدیل به Map Drive خواهد شد، برابر خواهد بود حجم کامل Drive D سیستم File Server !
حال اگر بخواهیم حجم این پوشه را کنترل کنیم؛ از ابزار Quota Management استفاده می کنیم.
می بینیم که شامل دو آبجکت می باشد.

- Quota Templates : شامل یک سری نمونه ی آماده ی «تعریف محدودیت» است که می توان از آنها استفاده کرد. می توانیم روی آن کلیک راست کرده و Create Quota Template را بزنیم.
  - یک نام برای آن درج می کنیم.
  - در قسمت Space Limit میزان مجاز موردنظر را درج می کنیم.
  - با انتخاب Hard Quota، به هیچ وجه اجازه ی گذر از میزان تعیین شده را به کاربر نمی دهد.
  - با انتخاب Soft Quota، اجازه ی گذر از میزان تعیین شده را می دهد، اما در ادامه باید دلیل آن بررسی شود.
  - قسمت Notifications Thresholds برای حالت Soft است که تعیین می کند، اگر از استفاده از میزان فضایی که تعیین شده، از یک یا چند مختلف بیشتر شود، چگونه اطلاع دهد. و تمام و OK!
- Quotas : محدودیت های تعریف شده برای پوشه ها، درون این آبجکت ایجاد می شوند که روی آن کلیک راست کرده و Create Quota را می زنیم.
  - برای Quota Path، پوشه ای که قصد مدیریت فضای آن را داریم انتخاب می کنیم.
  - برای اینکه Quota ی ایجاد شده، هم روی آن پوشه و هم روی زیرپوشه های آن اعمال شود، گزینه ی Auto apply template and create quotas را می زنیم.
  - در قسمت ...Device properties from this quota ، گزینه ی Quota Template ای که ایجاد کرده بودیم را انتخاب می کنیم.
    نکته: می توان یکی از Templateهای آماده را (با حجم های مشخص شده)، نیز انتخاب کرد.
  - و تمام و OK!
- حال به سادگی می توان این پوشه را در شبکه Share کرد، بدون آنکه نگران استفاده ی غیرقابل انتظار کاربرها از حجم آن و در نتیجه پر شدن درایو موجود در File Server باشیم.

: Disk Implementieren

- در ابتدا با دستور زیر می توانیم زیر می توانیم تمامی دستورات مربوط به **Storage** ها را مشاهده کنیم:

```
Get-Command -Module Storage
```

- توسط دستور زیر می توانیم همه ی دیسک های متصل به سیستمی که فعال هستند را با مشخصات، مشاهده کنیم:

```
Get-Disk
```

- با دستور زیر، می توانیم همه ی دیسک های فیزیکی متصل به سیستم را با مشخصات، مشاهده کنیم:

```
Get-PhysicalDisk
```

نکته: **Disk** هایی که **Partition Style** شان به صورت **RAW** است، یعنی هنوز خام و فاقد **Partition Table** بوده و قابل استفاده نیستند.

- توسط دستور زیر، **Partition** های فعال و حاضر سیستم را، مشاهده می کنیم، طوری که نشان می دهد هر **Partition** از کدام **Disk** است:

```
Get-Partition
```

در قسمت **Size Type**، **حجم قابل استفاده** و احتمالاً **حجمی که توسط سیستم اشغال و Reserve** شده را می بینیم.

اما حجمی که توسط کاربر استفاده شده و حجم خالی (باقیمانده) را نمی بینیم!

- اما توسط دستور زیر، می توانیم همه ی **Volume** ها (**Drive** هایی که در **My Computer** هستند) را همراه با فضای استفاده نشده را ببینیم:

```
Get-Volume
```

- برای اینکه یکی از دیسک های **RAW** را متصل و راه اندازی کنیم، توسط شماره ی آن در دستور زیر، دستور زیر را وارد می کنیم:

```
Initialize-Disk -Number 3 -PartitionStyle GPT
```

- توسط دستور زیر، برای یک **Disk** که **Initialize** شده و فعال است، یک **Partition** ایجاد می کنیم:

```
New-Partition -DiskNumber 3 -UseMaximumSize -DriveLetter G
```

توسط فرمان **UseMaximumSize**، درخواست می کنیم که همه ی حجم این دیسک را به این **Partition** اختصاص بدهد.

حال **Partition** ایجاد شده، هنوز فعال نیست، چون فاقد **File System** و **Name** و میزان **AUS** است. یعن **Format** نشده است.

- توسط دستور زیر، **Partition** فعال شده را، **Format** و راه اندازی می کنیم:

```
Format-Volume -DriveLetter U -FileSystem ReFS -AllocationUnitSize 4096 -NewFileSystemLabel "my_Datas"
```

- حال فرض کنید دیسک های زیادی داریم، و می خواهیم همه ی آنها را همزمان و یکباره، **initialize** کرده و یک **Partition** برای آنها ساخته و آن را **Format** و راه اندازی کنیم:

```
Get-Disk | Where-Object PartitionStyle -EQ "RAW" | Initialize-Disk -PartitionStyle GPT -PassThru | New-Partition
-UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem ReFS -AllocationUnitSize 65536 -Confirm
```

: Virtual Disk Implementieren

از طریق کنسول Disk Management :

- در منوی بالا، وارد Action شده و Create VHD را می زنیم.
- از طریق Browse جایی و نامی برای ذخیره سازی آن تعیین می کنیم. سپس حجم و مشخصات را تعیین و OK می کنیم.
- می بینیم که به لیست دیسک ها در همین کنسول اضافه شده است، که به سادگی آن را Initialize و فعال می کنیم.

یکی از ویژگی های مهم این Virtual Disk ها Portable بودن آنهاست. برای اینکه این دیسک را جدا کرده و به جایی دیگر منتقل کنیم:

- بر روی نام این دیسک در همین کنسول، کلیک راست کرده و Detach VHD را می زنیم.
- برای بازگرداندن آن و یا متصل کردن یک VHD دیگر به سیستم، کافی ست از منوی بالا و Action گزینه ی Attach VHD بزنیم.

از طریق کنسول PowerShell :

نکته: از آنجایی که دستورات کار بر روی VHD مربوط به Hyper-V هستند، ابتدا باید سرویس Hyper-V را نصب و راه اندازی کرده باشیم.

- توسط دستور زیر، می توانیم تمامی دستورات Hyper-V که مربوط به VHD باشند را ببینیم:

```
Get-Command -Module Hyper-v -Name *vhd*
```

- برای ایجاد VHD، دستور زیر را وارد می کنیم:

```
New-VHD -Path f:\VHard.vhdx -SizeBytes 70GB -Dynamic
```

- توسط دستور زیر، آن را به دیسک های سیستم، Attach می کنیم:

```
Mount-VHD -Path f:\VHDP.vhdx
```

- برای دریافت مشخصات یک VHD، از دستور زیر استفاده می کنیم:

```
Get-VHD -Path f:\VHDP.vhdx
```

چون اولین بار است که آن را mount می کنیم، هنوز Initialize و قابل بازشدن نیست.

- توسط دستورات زیر، ابتدا شماره ی این Disk را پیدا کرده و سپس آن را Initialize می کنیم:

```
Get-Disk
Initialize-Disk -Number 5 -PartitionStyle GPT -PassThru | New-Partition -UseMaximumSize
-AssignDriveLetter | Format-Volume -FileSystem NTFS
```

- می توانیم درون این VHD فایل ذخیره و حذف کنیم و سپس یا روی آن کلیک راست و Eject را بزنیم و یا توسط دستور زیر، آن را از سیستم جدا کنیم:

```
Dismount-VHD -Path f:\VHDP.vhdx
```

نکته:

پس همانطور که می دانیم، از این VHD ها هم می توان یک Virtual Machine ایجاد کرد و هم به عنوان یک Partition آن را Attach کرد. اگر در یکی از این موارد متصل باشد، در مورد دیگر نمی تواند متصل شود!

:(Redundant Array of Independent Disks) RAID

اگر بیش از یک دیسک Dynamic داشته باشیم، می توان Volume ها را به چند روش پیکربندی کرد، که این روش ها همگی، نوعی Raid هستند.

Raid به معنی آرایه ی اضافه شده ی دیسک های مستقل می باشد.

- چندین Dynamic Disk با هم ترکیب می شوند و یک Array پدید می آید.
- دلیل استفاده از تکنولوژی RAID این است که با قرار دادن داده ها بر روی بیش از یک عدد Disk، عملیات I/O ، به یک پوشش و پاسخگویی خاصی می‌رسد که نتیجه ی آن افزایش سرعت خواندن و نوشتن است.
- سیستم‌عامل، هاردهای RAID شده را به عنوان یک Disk تنها، شناسایی خواهد کرد.
- RAID چندین دیسک سخت را در یک آرایه، جهت بهبود و افزایش حجم موجود و کارایی و امنیت، گرد هم می آورد.
- اهداف استفاده از فناوری RAID :
  - افزایش توان کاری (Performance)
  - افزایش تحمل در برای خرابی (Fault-Tolerance)

دو نوع Raid وجود دارد: سخت افزاری و نرم افزاری.

- Raid سخت افزاری، کنترل و قدرت بسیار بالاتری دارد.
- در Raid سخت افزاری، داده ها از Disk ها، به یک کنترل کننده انتقال می یابند، به نام Raid Controller.
- RAID Controller، وظیفه ی مدیریت و کنترل Disk های متصل شده را برعهده دارد.
- این کنترلر هوشمند به دو شکل internal و external وجود دارد.
- مدل internal در داخل سیستم Server و به mainboard متصل می‌شود.
- مدل external، در شبکه های بزرگتر به کار می‌رود.

معایب Hardware Raid:

- افزایش هزینه
- در صورتی که RAID Controller با مشکل مواجه شود، تا زمان رفع مشکل و یا جایگزین کردن کنترلر جدید، دسترسی به اطلاعات دیسک‌ها نیز امکانپذیر نخواهد بود.

مزایای Hardware Raid:

- در Hardware Raid نیازی نیست که CPU درگیر محاسبات شود و این عملیات توسط Raid controler انجام می‌شود.
- اغلب RAID Controller ها جایی برای افزودن باتری دارند که درهنگام قطع ناگهانی برق، اطلاعات از دست نروند.
- Hardware Raid، قابلیت Hot Swapping است.

- در مواقعی که سیستم، Raid سخت افزاری را پشتیبانی نمی کند، و یا اینکه حجم داده ها، زیاد نیست، از Raid نرم افزاری استفاده می کنیم.
- اجرای Task ها و مدیریت Volume ها، همگی توسط CPU صورت می شود، پس وابسته به قدرت CPU و میزان load آن می‌باشد.
- Software Raid وابسته و محدود به سیستم عاملی است که بر روی آن ایجاد شده است. یعنی اگر RAID را به یک سیستم عامل دیگر ببریم، شناسایی نخواهد شد.

- جهت راه اندازی RAID نرم افزاری:
  - نرم افزارهایی وجود دارند که می توان نصب و استفاده کرد.
  - می توان از کنسول Disk Management که به صورت پیشفرض این فناوری را پشتیبانی می کند، استفاده کرد.

Spanning یا NRaid:

تمام فضاهای ذخیره سازی مربوط به چند دیسک **Dynamic**، فقط به یک **Volume** تبدیل می شوند، که آن را **Spanned Volume** می نامند.
در این روش، اطلاعات به ترتیب در دیسک ها ذخیره می شوند. یعنی ابتدا، اولین دیسک پر می شود، سپس دیسک بعدی و ... .
این عمل تا وقتی که کل فضاهای ذخیره سازی به طور کامل پر شود، ادامه پیدا می کند. هدف از این روش، دسترسی به کل فضای ذخیره سازی، از طریق یک **volume** می باشد.

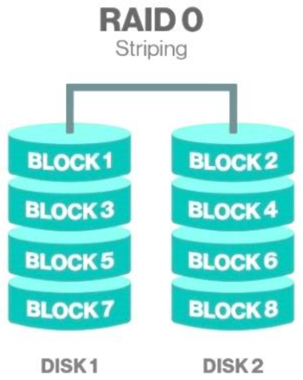
- می‌توان تا **32** دیسک را طبق این روش، عضو **Volume** کرد.
- برای ایجاد اینگونه از **Volume** ها، **File System** دیسک ها باید **NTFS** باشد.
- به این تک ولومی، **Spanned Volume** و یا **JBOD** (**Just a Bunch Of Disks**) گفته می شود.

Striping یا RAID 0 :

در این روش:

- ✓ باید حداقل دو Disk داشته باشیم.
- ✓ **امنیت نگهداری اطلاعات، در پایین ترین سطح قرار دارد، چون اگر فقط یکی از دیسک ها از کار بیفتد، همه ی اطلاعات از بین می روند.**
- ✓ **سرعت ذخیره و بازیابی داده، در بالاترین سطح قرار دارد.**
- ✓ **فضای قابل استفاده در هر Disk، محدود به اندازه ی فضای کوچکترین دیسک عضو همبندی یا Raid خواهد بود.**
  مثلاً اگر سه دیسک با حجم های 60 و 80 و 120 گیگابایت داشته باشیم، فضای قابل استفاده از هر دیسک، محدود به 60 GB می شود.
  پس درنهایت، کل فضای موجود، 180 گیگابایت خواهد بود.
- ✓ **بهتر است که دیسکها، هم ظرفیت و حتی دارای مشخصات فنی یکسان باشند، تا هیچ مقداری از فضای Disk ها، بی استفاده نماند.**
- ✓ **اطلاعات به صورت قطعه های Striped یا راه راه که هریک 64 کیلوبایت حجم دارند، در حافظه ذخیره می شوند.**
- ✓ **و خواندن و نوشتن اطلاعات، از روی همین قطعه های راه راه صورت می گیرند.**

- **Strip ها به صورت ترتیبی، پر می شوند. مثلاً File1 بر روی Disk1 و File 2 بر روی Disk2 و File3 بر روی Disk1 ذخیره می شود.**
- **Striping باعث شده که این روش، به عنوان سریع ترین و پرگنجایش ترین RAID شناخته شود.**



معایب RAID 0 :

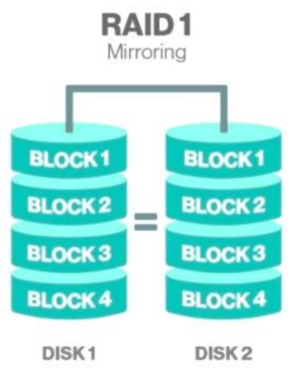
- **بازیابی اطلاعات در این Raid به دلیل تقسیم داده ها میان تمام Disk ها، بسیار مشکل می باشد.**
- **اگر داده ای فقط در یکی از Disk ها به مشکل برخورد کند، تمام داده های Disk های دیگر هم از دست خواهند رفت.**
- **پس این Raid، فاقد Fault Tolerance یا قدرت تحمل خطا می باشد.**

Mirroring یا RAID 1 :

فناوری این نوع RAID بسیار ساده می باشد.

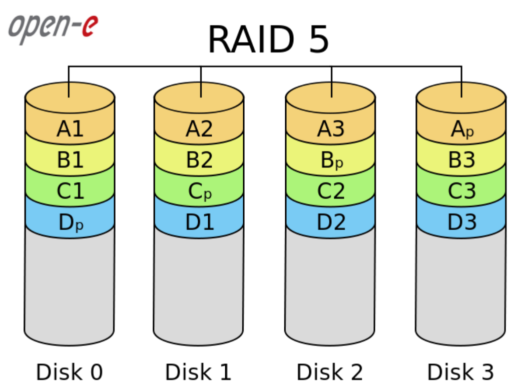
در این Raid:

- ✓ **اطلاعات به صورت همزمان و کاملاً مشابه، بر روی Disk ها نوشته می شوند.**
- ✓ **به عنوان مثال اگر 4 هارددیسک را با این روش RAID کنیم، دو Disk، تبدیل به کپی هایی از داده های دو Disk دیگر می‌شوند.**
- ✓ **تعداد هارد دیسک ها در این Raid، باید زوج باشد.**
- ✓ **در این RAID اطلاعات همزمان می‌توانند از روی هر دو Disk خوانده شوند، پس سرعت Read در این ساختار بالاست. اما سرعت Write در این ساختار، کمتر است، چون هر داده باید دوبار نوشته شود.**
- ✓ **روشی گران قیمت، اما امن است. چون داده ها بر روی هر دو یا چند Disk قرار دارند، سطح Availability بالا می رود، به این صورت که اگر یکی از دیسک ها down شود، Disk دیگر بالا آمده و هیچ داده ای از بین نمی رود.**
- ✓ **در این روش نیز بهتر است که دیسکها، هم ظرفیت و دارای مشخصات فنی یکسان باشند.**
- ✓ **این نوع RAID، تنها نوعی هست که در آن، برای تعویض یک دیسک عضو Raid و یا افزودن یک دیسک جدید به Raid، نیازی به خاموش کردن سیستم نخواهد بود، هرچند که در همه ی Raid ها، برای تعویض یا افزودن یک دیسک، پیشنهاد می شود ابتدا Server خاموش شود.**



Striping with Parity or RAID 5 :

- ✓ به آن نواربندی با بیت افزونه هم گفته می شود.
- ✓ **این Raid رایج ترین نوع RAID می باشد.**
- ✓ **بر روی Windows Server قابل استفاده است.**
- ✓ **حداقل نیازمند به 3 دیسک می باشد، که می توان آنرا تا 16 عدد نیز افزایش داد.**
- ✓ **برای افزایش کارایی، توصیه می شود که حداقل از 5 دیسک استفاده شود.**
  مانند RAID 0، داده ها در نوارهایی 64 کیلوبایتی و در تمامی دیسک ها نوشته می شوند، و باز هم Data به صورت یکنواخت بر روی یک دیسک نمی باشد، بلکه در تمام دیسک ها پخش می باشد.

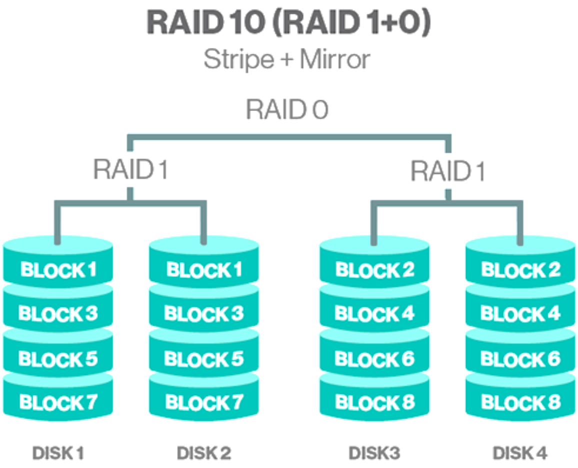


- ✓ **اما تفاوت اصلی این RAID با RAID 0، این است که اطلاعاتی با نام Parity همراه با این نوارهای 64 کیلوبایتی در دیسک ها ذخیره می شوند تا اگر یکی از Disk ها آسیب ببیند، سیستم با استفاده از اطلاعات باقی مانده و اطلاعات Parity، اطلاعات دیسک آسیب دیده را بازسازی کند.**
- ✓ **البته این عملیات بازیابی، زمان زیادی لازم خواهد داشت.**

- ✓ **سرعت پایینی برای ذخیره ی داده ها دارد، چون عملیات تولید Parity هم تا حدی زمان‌بر است.**
- ✓ **اما برای Read، سرعت خوبی دارد، به همین جهت، در مورد آن گفته می شود:** Write one, Read many!
- ✓ **به همین جهت، برای ذخیره سازی فایل های stream مثل ویدیو و موسیقی مورد استفاده قرار می گیرد.**
- ✓ **پس RAID 5 برای سیستم‌هایی که عملیات نوشتن زیاد و فشرده دارند، اصلا گزینه ی مناسبی نیست، اما برای پایگاه داده ها مثل SQL مناسب است.**
- ✓ **ترتیبی که دیسک ها را روی Server سوار می کنیم، آنقدر مهم است که اگر جای دو دیسک را با هم عوض کنیم، Raid خراب خواهد شد.**
- ✓ **اگر یکی از Disk ها به هر دلیلی دچار مشکل شود،** (یا حتی به عمد یکی از دیسک ها را از جای خود قطع و خارج کنیم) **سیستم بدون هیچ وقفه ای، به کارخود ادامه می دهد تا اینکه یک Disk جدید روی Server قرار داده شود و سپس داده ها روی آن شروع به Recover شدن می‌کنند.** (اما اگر دو دیسک را از Raid جدا کنیم، دیگر قابل Recover شدن نخواهند بود و Raid خراب می شود.)

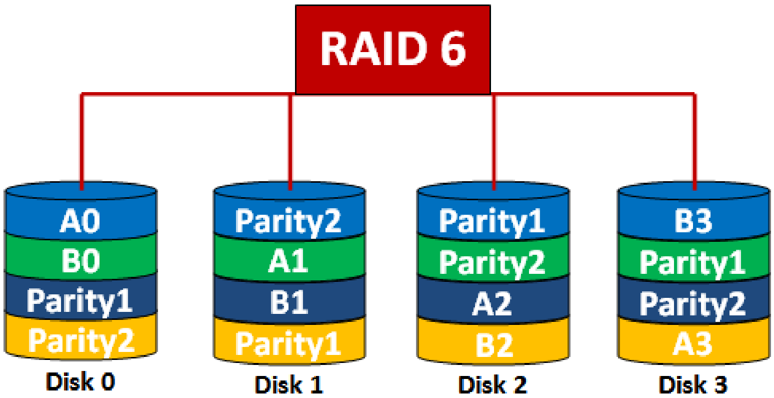
: RAID 10

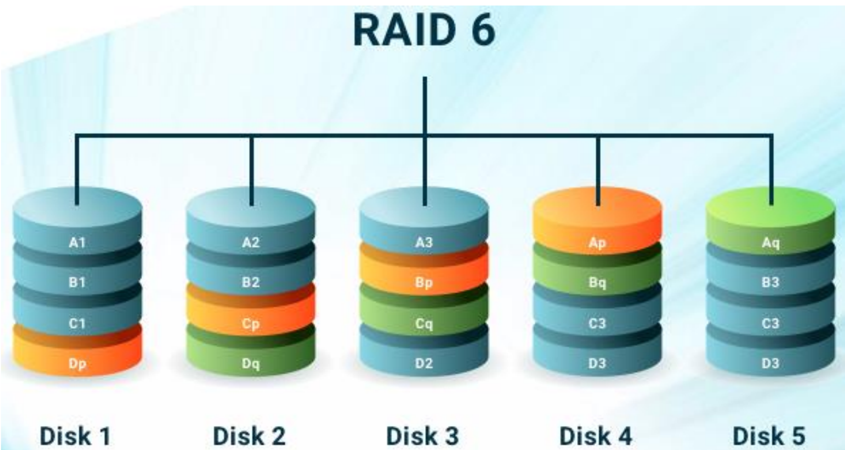
- ✓ همانطور که در تصویر دیده می شود، این RAID ترکیبی از RAID های صفر و یک می باشد.
- ✓ این RAID هم دارای سرعت بالای RAID0 و هم دارای Fault Tolerance مربوط به RAID1 می باشد.
- ✓ اگر در شبکه speed و redundancy را همزمان بخواهیم، از این RAID استفاده می کنیم.



: RAID 6

- ✓ حداقل نیازمند به 4 دیسک می باشد.
- ✓ **اگر دو Disk عضو RAID، به هر دلیلی دچار مشکل شوند،** (یا حتی به عمد دو دیسک را از جای خود قطع و خارج کنیم) **سیستم بدون هیچ وقفه ای، به کارخود ادامه می دهد تا اینکه دو Disk روی Server قرار داده شوند و سپس داده ها روی آن شروع به Recover شدن می‌کنند.**





:RAID Comparison

همیشه و در هر **Raid** ای، سرعت **Read** از سرعت **Write** بیشتر است.

RAID Level	Read Speed	Write Speed	Fault Tolerance	Min. used Disks	Fault Tolerance
RAID 0	fastest	fastest	zero	2	0
RAID 1	slowest	slower	highest	2	1
RAID 5	faster than RAID 1	slower than RAID 1	medium	3	1
RAID 6	faster than RAID 5	slower than RAID 5	high	4	2
RAID 10	fastest	faster than RAID 5	highest	4	2

: Storage Pool

Tiered Storage روشی برای اختصاص دادن داده های دسته بندی شده به انواع مختلف **Storage** می باشد، با هدف کاهش هزینه!
یا به عبارتی، یک تکنیک ذخیره سازی شبکه ای است که این ذخیره سازی، بر روی انواع مختلف رسانه ها انجام می شود.

- به طور معمول **Tiered** ها با توجه به هزینه ی **Storage** ها، تعیین می شوند.
- **Data** ها با توجه به حجم درخواست کاربران برای آنها، رتبه بندی می شوند.
- به طور کلی، ذخیره ی مهمترین **Data** ها، در سریع ترین **Storage** ها که معمولا گران ترین هم هستند، انجام می شود.
- در حقیقت در روش **Tiering**، مکان ذخیره سازی داده ها تغییر می کند.

فرض کنید که حجم معینی از داده ها را داریم، و طبق تجربه، می دانیم که :
- بخش کمی از داده ها به صورت **hot** می باشند، یعنی درخواست دسترسی به آنها بسیار زیاد می باشد،
- بخشی از داده ها به صورت **Warm** هستند که درخواست دسترسی به آنها معمولی می باشد،
- بخش بیشتری از داده ها **cold** هستند که بسیار کم به آنها درخواست دسترسی وجود دارد.

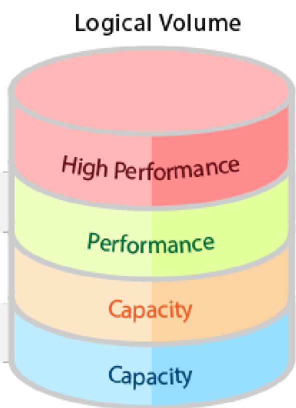
برای **Tiered Storage** همینقدر کافی ست.

- **Tiered Storage** توسط **Life-cycle Management** (مدیریت چرخه ی حیات) از **Data Corruption** (گم شدن و نابودی اطلاعات) جلوگیری می‌کند.

Tiered storage طیفی از زیرساخت‌ها را در بر می‌گیرد، مثل:
- معماری **Two-Tiered** (دو لایه ای) که شامل **SCSI** و **Fiber Channel Attached Disk** می باشد.
- زیرساخت‌های پیچیده‌تری که شامل پنج یا شش **Tiered** هستند.

: Automated storage tiering

عبارت است از فرآیند خودکارسازی ذخیره ی اطلاعات بر روی **Storage** های متفاوت یا **Tier** های مختلف.
اگر نیاز بود که اطلاعات مداوم در دسترس باشند، اطلاعات بر روی **Tier** های بالاتر ذخیره خواهند شد، مثل **Tier1** یا **Tier 2** و اطلاعاتی مثل **Backup** ها و بایگانی ها، بر روی **Tier** های پایین تر که ظرفیت بیشتر و سرعت دسترسی پایین تری دارند، ذخیره خواهند شد.
یک نرم افزار مسئولیت انجام این کار را دارد و به این عملیات **Automated Tiered Storage** می گویند.



	Access Rate	Recommended Drive Type	Recommended RAID Level
Tier0	Most Frequent	SSD	RAID1
Tier1	Frequent	SAS	RAID1
Tier2	Infrequent	NL-SAS	RAID5 or 6
Tier3	Rarely	SATA	RAID5 or 6

: implementation a Storage Pool

فرض کنید، شش دیسک را به سیستم متصل کرده ایم و هنوز هیچ کدام فعال یا initialize نشده اند.

- در PowerShell دستور زیر را وارد می کنیم:

```
Get-PhysicalDisk
```

- برای ستون CanPool می بینیم که مقدار true قرار دارد، این یعنی اینکه این Storage ها هنوز به هیچ Pool ای متصل نشده اند و می توانند متصل شوند.
- به Server Manager و Files and Storage و سپس به Disks می رویم تا از صحت وجود دیسک ها مطمئن می شویم و سپس به تب Storage Pool می رویم.

نکته: اگر دیسک جدیدی، به سیستم اضافه کرده باشیم، اما در این تب، گزینه ای به نام Primordial برای آن اضافه نشده باشد، از طریق گزینه ی Tasks در بالا سمت راست، یکبار Rescan را می زنیم.

1. یک Storage Pool ایجاد می کنیم.

- در تب Storage Pools بر روی سطری که در زیر گزینه ی این Server به نام آن Primordial است، کلیک راست کرده و New Storage Pool را می زنیم. (و یا در بالا سمت راست، از طریق Task)
- یک نام برای آن درج می کنیم و next.
- همه ی دیسک ها را انتخاب می کنیم و در پایان Create.

نکته: وقتی یک دیسک، عضوی از یک Pool می شود، مقدار CanPool برای آن دیسک، false خواهد شد.

نکته: در این مثال، اگر بر روی سیستمی مجازی ساز مثل VMware باشیم، نیاز است که پس از عضو کردن Disk ها در Pool، نوع Storage ها را به HDD یا SSD تغییر دهیم.

- ❖ پس ابتدا توسط دستور زیر، نوع Storage ها را مشاهده می کنیم:

```
Get-PhysicalDisk | ft size,mediatype,deviceid
```

- ❖ برای تغییر آنها به SSD یا HDD دستور زیر را برای هریک از deviceID های مورد نظر وارد می کنیم:

```
Get-PhysicalDisk | where deviceid -EQ 2 | Set-PhysicalDisk -MediaType HDD
```

نکته: جهت کار با Tiered Storage، برخی ها را SSD و برخی را HDD قرار می دهیم، چون اگر همه یک نوع باشند، نمی توان Tiered داشت.

- ❖ دوباره به Server Manager و Storage Pool رفته و یکبار Refresh می کنیم.

ایجاد Storage Pool در PowerShell:

```
New-StoragePool -FriendlyName MyPool -StorageSubSystemUniqueId (Get-StorageSubSystem).UniqueId -PhysicalDisks (Get-PhysicalDisk -CanPool $true)
```

تفسیر:

- ابتدا نیاز به Unique ID مربوط به سیستم جاری داریم که StorageSubSystemuniqueID نامیده شده و یک عدد طولانی است:
  توسط Get-StorageSubSystem، مشخصات سیستم جاری را پیدا می کنیم، و به آن سوییچ uniqueID را وصل می کنیم.

```
(Get-StorageSubSystem).UniqueId
```

- سپس نیاز به انتخاب Disk های مناسب برای Pool موردنظر داریم.
  توسط دستور زیر، در می یابیم که کدامیک از Disk های متصل به سیستم، آماده و قادر به عضویت در یک Pool هستند:

```
Get-PhysicalDisk -CanPool $true
```

2. یک Disk مجازی از بخشی و یا از تمام Pool ای که ساختیم، ایجاد می کنیم.

- حال بر روی Pool ای که ایجاد کردیم، کلیک راست کرده و New Virtual Disk را زده و Ok و Next.
- یک نام برای آن درج کرده و تیک گزینه ی Create storage tiers را فعال می کنیم.

Enclosure :

به طول معمول نوعی جعبه یا **Case** یا محفظه ی آماده است که شامل چندین **disk** می باشد.

این **Disk** ها می توانند به صورت **JBOD** تنظیم شده باشند.



- در صورتی که در شبکه، حداقل یک **Enclosure** داشته باشیم، می توان گزینه ی **Enable enclosure** را فعال کرد.
- یکی از گزینه های **Simple** یا **Mirror** را انتخاب می کنیم، اگر **Tiers** را فعال نکرده بودیم، **Parity** هم قابل انتخاب می بود.
- در حقیقت در اینجا اگر گزینه ی **Storage Tiers** را فعال نکرده بودیم، می توانستیم، **Thin** را انتخاب کنیم، که مثل حالت **dynamic** برای **VHD** ها عمل می کند، و می تواند مقداری بیش از فضای موجود دیسکها باشد.
  اما در حالت **Tiers**، باید به صورت **Fixed** عمل کرده و همه ی فضای **Disk** های معرفی شده را یکجا اختصاص بدهد.
- در تب **Size**، می توانیم برای **Disk** های سریع تر (**Faster**) و دیسک های کُندتر (**Standard**) تعیین کنیم که چه مقدار از فضای آنها را استفاده کند، و یا اینکه تمام فضای آنها را بدهد.
- پس از **Create** و قبل از **Close**، می توانیم فعلاً **... Create a volume when this** را غیرفعال کنیم.
- می بینیم که **Virtual Disk**، در پایین سمت چپ ایجاد شده است. و در بالا، می توان به بخش **Disks** رفته و یا وارد کنسول **Disk Management** رفته و گزینه ی آن را مشاهده کرد.

ایجاد Virtual Disk از یک Storage Pool، توسط PowerShell:

```
New-VirtualDisk -FriendlyName myData -StoragePoolFriendlyName MyPool -Size 270GB -ProvisioningType Thin
-ResiliencySettingName simple
```

سپس این **Disk** را **initialize** می کنیم:

```
Initialize-Disk -VirtualDisk(Get-VirtualDisk -FriendlyName myData)
```

3. از این Disk جدید، حداقل یک Partition جدید ایجاد می کنیم.

- پس در همین **Server Manager** بر روی آن، کلیک راست و **New Volume** را می زنیم و تا پایان پیش می رویم.

ایجاد Volume از یک Virtual Disk، توسط PowerShell:

ابتدا باید خود **Virtual Disk** را انتخاب کنیم و سپس، جهت انجام عملیات، مثل یک دیسک فیزیکی آن را انتخاب و یک **Partition** از آن ایجاد کرده و آن **Partition** ها را یکی یکی **Format** کنیم:

روش اول:

```
Get-VirtualDisk -FriendlyName myData | Get-Disk | New-Partition -Size 270GB -AssignDriveLetter
```

نکته: به جای **Size-** می توانیم از **UseMaximumSize-** استفاده کنیم.

حال که یک **Partition** را اضافه کردیم، مشخصات **Partition** های سیستم را یکبار می بینیم:

```
Get-Partition
```

Partition جدید را انتخاب و **Format** می کنیم:

```
Get-Partition -PartitionNumber 2 | Format-Volume -FileSystem NTFS -AllocationUnitSize 4096
```

روش دوم:

```
Get-VirtualDisk -FriendlyName myData | Get-Disk | New-Partition -Size 270GB -AssignDriveLetter | Format-Volume -FileSystem
NTFS -AllocationUnitSize 4096
```

همانطور که می بینیم، انتخاب یک دیسک مجازی و انتخاب آن دیسک جهت انجام عملیات بر روی آن و ایجاد Partition و Format کردن، مراحلی گوناگون هستند، که می توان با Pipe، آنها را از یکدیگر جدا کرد، اما همزمان انجام داد.

روش سوم:

هردو مرحله ی انتخاب Disk را درون یک متغیر ذخیره می کنیم:

```
$myVHD = Get-VirtualDisk -FriendlyName myData | Get-Disk
```

```
$myVHD | New-Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem NTFS -AllocationUnitSize 4096
-NewFileSystemLabel "forBackup"
```

4. اضافه کردن دیسک های جدید به سیستم:

فرض کنید بعد از مدتی، تصمیم گرفتیم و دو Disk جدید به سیستم یا به Exclosure متصل به این Pool، اضافه کردیم.

برای افزودن آنها به فضای Pool، کافی ست به Server Manager و تب Storage Pools برویم، و یکبار Refresh کنیم:

- بر روی گزینه ی مربوط به Pool، کلیک راست کرده و Add Physical Disk را می زنیم.
- هر دو دیسک را انتخاب کرده و OK!
- در همین تب Storage Pools، در پایین سمت چپ، بر روی Virtual Disk کلیک راست کرده و Extend virtual Disk را زده و حجم اضافه شده را درج و OK می کنیم.
- به تب Volumes رفته و بر روی Partition موردنظر کلیک راست کرده و Extend Volume را می زنیم.

: Troubleshooting the Storage Pool

:Remove

- برای حذف همه ی **Volume** های این **Disk**، کافی ست در **Server Manager** و در تب **Disks**، بر روی خود **Disk** کلیک راست کرده و **Reset Disk** را بزنیم.
- برای حذف **Virtual Disk**، وارد تب **Storage Pools** شده و در پایین، سمت چپ، روی آن کلیک راست کرده و **Delete** را می زنیم.
- برای حذف **Storage Pool** ایجاد شده، در همین تب **Storage Pools** و در بالا، روی آن کلیک راست و **Delete** را می زنیم.

- حال اگر به تب **Disks** برگردیم و یکبار **Refresh** کنیم، در زیرمجموعه ی گزینه ی این **Server**، می بینیم که همه ی دیسک ها لیست شده اند و نوع **Partition** همه آنها، **GPT** است. اگر بخواهیم دوباره یک **Pool** ایجاد کنیم، باید آنها را به حالت **Unknown** بازگردانیم. پس روی تک تک آنها کلیک راست کرده و **Reset Disk** را می زنیم.

: Defective Hard Drives

1. **دیسک های خراب یا از کار افتاده را پیدا می کنیم.**

نکته: با توجه به اینکه در سیستم های **Server** و یا **Enclosure** ها، دیسک های زیادی را به طور مشابه راه اندازی می کنیم، پیدا کردن، شماره **Slot** یا مکان **Disk** مهم است، پس از گزینه ی **physicallocation** هم استفاده می کنیم.

```
Get-PhysicalDisk | sort -Property size
Get-PhysicalDisk | ft deviceid,friendlyname,serialnumber,size,physicallocation
Get-PhysicalDisk | Where HealthStatus -EQ warning
Get-PhysicalDisk | Where healthstatus -ne Healthy

      Get-PhysicalDisk |ft friendlyname
```

فرض می کنیم که دیسکی فیزیکی به نام **Generic Physical Disk** که عضو **Virtual Disk** به نام **MyVDisk** و عضو**Pool** به نام **myPool** می باشد، خراب شده باشد.

2. **دیسک های معیوب را بازنشسته می کنیم.**

ابتدا به آنها، برچسب بازنشسته می زنیم؛ پس مقدار **Usage** آنها را به **Retired** تغییر می دهیم:

```
Set-PhysicalDisk -FriendlyName "Generic Physical Disk" -Usage Retired
```

3. **دیسک مجازی را تعمیر می کنیم.**

برای اطمینان، دوباره نام **Virtual Disk** ها را پیدا کرده و تک به تک آنها را تعمیر می کنیم:

```
Get-VirtualDisk
Repair-VirtualDisk -FriendlyName " MyVDisk"
```

برای اطمینان از پایان تعمیر موفقیت آمیز، می توانیم توسط دستور زیر، آن را بررسی کنیم:

```
Get-StoragePool
```

4. فرآیند [انتخاب دیسک های معیوب] را در یک متغیر قرار می دهیم:

```
$R = Get-PhysicalDisk | Where-Object { $_.Usage -eq ‘Retired’}
```

5. دیسک های معیوب را از درون **Pool** حذف می کنیم.

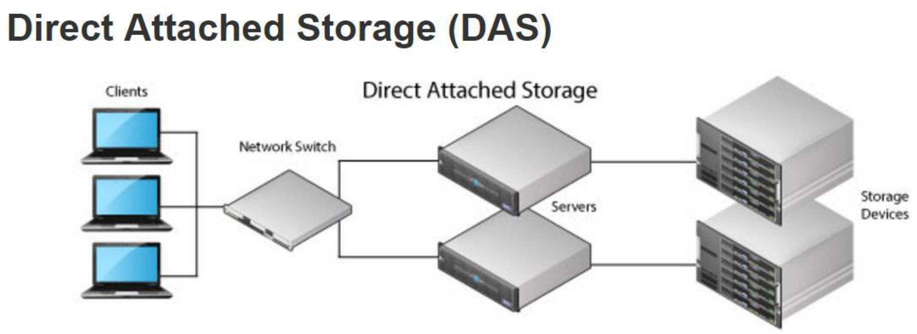
برای اطمینان، دوباره نام **Storage Pool** ها را پیدا کرده و همه ی دیسک های خراب را یکجا حذف می کنیم:

```
Get-StoragePool
Remove-PhysicalDisk -PhysicalDisks $R -StoragePoolFriendlyName "myPool"
```

: Hardware RAID

بطورکلی سه نوع Storage وجود دارد که می توان Hardware Raid را برای آنها پیاده سازی کرد:

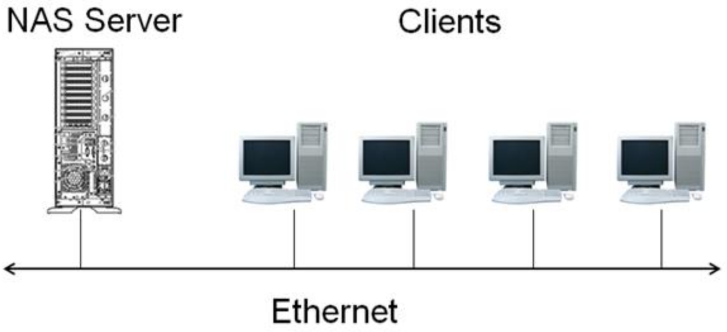
- **: (Direct Attached Storage) DAS**
  - در حقیقت قدیمی ترین نوع Storage می باشد.
  - هزینه ی پایین تر و راه اندازی ساده تری نسبت به انواع دیگر دارد.
  - همان Hard های external کوچکی که استفاده می کنیم هم DAS محسوب می شوند.
  - در حقیقت DAS یک Storage است که به صورت مستقیم به یک کامپیوتر متصل می شود.
  - Flash memory هم DAS است.
  - Hard Disk های PC و Laptop هم DAS محسوب می شوند.
  - بنابراین هر Storage ای که به صورت مستقیم به کامپیوتر وصل می شود و می توانیم به صورت مستقیم از فضای آن استفاده کنیم، یک DAS است.
  - Enclosure ها هم می توانند DAS باشند.
  - ارتباط DAS با سایر تجهیزات موجود در شبکه از طریق Server خواهد بود.
  - اگر به هر دلیلی، سروری که DAS به آن متصل است، از دسترس خارج شود، DAS و محتویاتش نیز قطع می شوند.
  - DAS معمولاً توسط یکی از کابلهای SAS یا SCSI به Server متصل می شود، البته توسط Fiber Channel (FC) هم می تواند.
  - رابط بین Server و DAS، معمولا HBA یا SCSI Controller است.
  - اتصال DAS، تنها به یک Server ممکن است، البته توسط برخی Controller ها، امکان اتصال به دو یا بیشتر Server هم وجود دارد.
  - اگر حجم فایل ها و پیچیدگی آنها زیاد شود، باید یک SAN یا NAS را جایگزین DAS کنیم.
  - DAS می تواند از همه ی پروتکل های ذخیره سازی استفاده کند: SATA، eSATA، SCSI، FC و ...



- **:(Network Attached Storage) NAS**
  - این Storage ، که در حقیقت یک Shared Storage است، مشابه به File Server، اما با پیچیدگی های کمتر.
  - مثل Client های شبکه، توسط یک Switch، به شبکه متصل می شود.
  - بطورمعمول به صورت یک Case در مکانی قرار می گیرد.
  - هم دارای سیستم عاملی سبک است و هم دارای کارت شبکه، به همین جهت توسط IP Address قابل دسترس هستند.
  - سیستم عامل آن معمولاً لینوکسی است، اما نسخه ی ویندوزی برای آنها، با نام Windows Storage Server موجود است.
  - همه ی کاربران عضو شبکه، به فایل ها و منابعی که بر روی NAS قرار دارند، دسترسی خواهند داشت.
  - پراکندگی اطلاعات را کاهش می دهد.
  - به تعداد نامحدودی از Client ها می توانند از آن Service دریافت کنند.

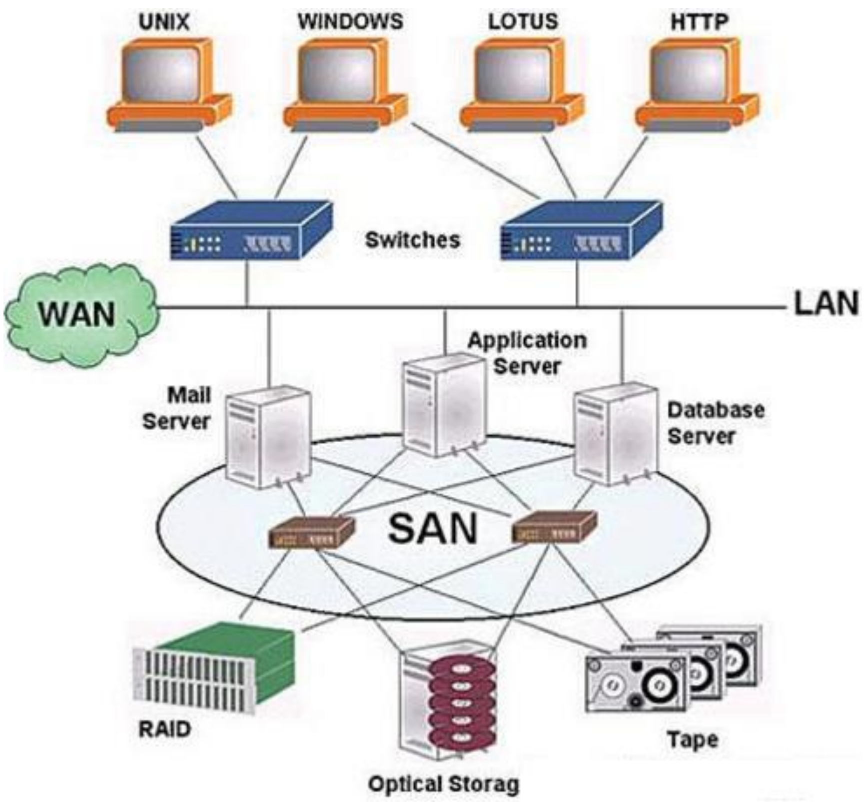
- اشتراک گذاری فایل ها را از طریق LAN یا WAN انجام می دهد.
- دیسک های مورد استفاده در NAS، دیسک های خاصی نیستند و از همان دیسک های سخت مشابه دیسک های موجود در کامپیوترهای دسکتاپ استفاده می کند.
- NAS وابستگی به نوع Server ها و سیستم عامل های آنها ندارد.

- هم پروتکل File Sharing سیستم های ویندوزی را پشتیبانی می کند، یعنی SMB، و هم پروتکل File Sharing سیستم های لینوکسی را پشتیبانی می کند، یعنی NFS.



- Control Panel مربوط به NAS ها، Web Base است. یعنی Admin، به صورت web base به آن متصل شده و Disk های آن را مشاهده کرده و می تواند آن ها را تنظیم کند.
- پس از Join شدن به Domain، در Active Directory برای آن Computer Account ساخته می شود.
- می توان درون آن Folder ایجاد و share کرد. و User های شبکه می توانند به NAS وصل شده و مثل یک File Server از آن استفاده کنند.
- Nas ها حداقل Raid های صفر و یک را پشتیبانی می کنند.
- NAS ها می توانند دو یا چند درگاه شبکه داشته باشند که سرعت های مختلفی را جهت اتصال به شبکه، پشتیبانی می کنند.
- NAS با یکی از دو پروتکل CIFS (برای شبکه های Windows) و NFS (برای شبکه های Linux)کار می کند.
- یکی از شرکت های خوب تولیدکننده ی NAS، شرکت QNAP می باشد.

- **SAN (Storage Area Network):**
  - در شبکه های بزرگ کاربرد دارد.
  - SAN می تواند شبکه ای از Storage ها باشد، که دارای یک SAN Switch برای اینکار خواهد بود.
  - بطورمعمول Rack Mode می باشد. (در Rack نصب می شود.)
  - دستگاه SAN دارای Flexibility، Availability و Performance بسیار بالاتری نسبت به DAS و NAS می باشد.
  - به Server وابستگی ندارد و بصورت مجزا می تواند در شبکه، کار کند. (توسط یک Switch، به شبکه وصل می شود.)
  - SAN مجموعه ای از دستگاه هاست که به خودی خود شبکه ای برای ذخیره سازی اطلاعات ایجاد می کنند، در حالیکه NAS فقط مجموعه ای از چند Disk است که با یک OS ساده در شبکه قابل دسترس بوده و هیچ پیچیدگی خاصی ندارد.
  - سرعت انتقال اطلاعات در SAN بسیار بالاتر از سرعت در DAS است.
  - بر روی یک SAN Storage می توان ارتباطات شبکه ای زیادی برقرار کرد.
  - کاربران با Storage ها، ارتباط مستقیم نخواهند داشت.
  - جهت راه اندازیِ SAN توسط SAN Switch، هم Storage ها و هم Server ها (مثل Mail Server، Application Server، Database Server و ...) را به SAN Switch متصل می کنیم؛ سپس Server ها را به فضای اصلی شبکه که شامل Client هاست، متصل می کنیم.
  - Storage های متصل به SAN Switch می توانند هم NAS باشند و هم DAS.
  - نسبت به NAS، دیسک های بیشتری را در بر خواهد گرفت، به همین جهت اندازه ی بزرگتری دارند.



- دو راه برای اتصال SAN به شبکه وجود دارد:

پروتکل‌های **iSCSI** (توسط پورت RJ45 و درگاه Ethernet) و **FiberChannel** (توسط درگاه های Fiber Channel)

وقتی با پروتکل‌های **iSCSI** کار می‌کنیم، دستگاه در سطح شبکه ی **Ethernet** فعال شده است، که نسبت به **FiberChannel** **قابلیت اعتماد و سرعت کمتر** و **راه اندازی ارزان** تری دارد، اما **انعطاف پذیری بیشتری** نسبت به **FC** دارد.

- وقتی با پروتکل **Fiber Channel** کار می کنیم، دستگاه در سطح شبکه ی **Optic Fiber** فعال شده است.
- راه اندازی آن گران تر است.
- اما پروتکلی هم به نام **FCOE** (**Fiber Channel Over Ethernet**) وجود دارد که بستر فیبر نوری را بر روی **Ethernet** فراهم می کند.

برای اتصال یک **Server** به شبکه ی **SAN** توسط درگاه **Fiber Optic**، باید روی **Server**، کارتی به نام **HBA** (**Host Bus Adapter**) نصب شود که این کارت با نام **FCA** (**Fiber Channel Adapter**) نیز شناخته می شود.

این کارت ها می توانند شامل یک و یا دو پورت باشند.

روی **HBA** یک آدرس فیزیکی به نام **WWN** (**World Wide Name**) وجود دارد.

شرکتهای **Qlogic** و **Emulex** دو شرکت مهم در زمینه ی تولید کارت **HBA** هستند.

هر اتصال **FC**، شامل دو مسیرِ رفت و برگشت است.

در شکل زیر یک **HBA** دو پورتی مشاهده می کنیم:



Storage Comparison :

- از لحاظ پیچیدگی راه اندازی، سخت ترین SAN و ساده ترین DAS است.
- از لحاظ کارایی برای شبکه، کارآمدترین SAN و ناکارآمدترین DAS می باشد.
- DAS، پایین ترین سرعت و SAN بالاترین سرعت را دارد.
- ساده ترین دسترسی را، NAS دارد.

iSCSI Storage :

فرض کنید یک شبکه دارای یک دستگاه **Storage** می باشد.

- هریک از **Disk** های درون **Storage** را **Target** و هریک از **Client** هایی که درخواست دسترسی به **Disk** های **Storage** را دارند، **Initiator** می نامیم.
- **Storage** ها دارای پروتکلی به نام **iSCSI** هستند که توسط آن، دسترسی به هریک از **Target** ها، به سادگیِ دسترسی به یک **DAS** خواهد بود.

ارتباط با **Storage** ها، بطور کلی بر پایه ی یکی از دو حالت زیر هستند:

- **File Base :**

بطورمعمول برای **NAS** استفاده می شود.

ارسال اطلاعات بصورت **File** پشت **File** انجام می شود.

- **Block Base (Block Level):**
  - به این صورت است که **Data** در **Block** هایی بدون فرمت منتقل می شود.
  - بطورمعمول برای پروتکل های **iSCSI** استفاده می شود.
  - سرعت و قابلیت های بیشتر و بالاتری دارد.
  - **DAS** و **SAN** بر این اساس کار می کنند.

iSCSI Target :

اگر بخواهیم در یک شبکه، چندین **Disk** را بدون یک دستگاه **Storage** مثل **SAN**، در شبکه به اشتراک بگذاریم، از پروتکل **iSCSI** در یک سیستم **Server** استفاده می کنیم، که **iSCSI Target** نامیده خواهد شد.

- ✓ **iSCSI Target** این امکان را فراهم می کند که بتوان بر روی شبکه های بر حسب **IP**، قابلیت **SAN** را راه اندازی کنیم.
- ✓ این قابلیت، نسبت به **Storage** های **SAN** :
  - سرعت کمتری دارد.
  - **Performance** پایین تری دارد.
  - برای شبکه های کوچک، کارآمد می باشد.
  - از آنجایی که سرعت شبکه را کاهش می دهد، باید مسیرها و طراحی شبکه را بطور بهینه انجام دهیم؛ مثلاً نصب و کابلکشی های آن، جدا از زیرساخت اصلی شبکه باشد.

- باید درون **iSCSI Target** تعریف کنیم که کدامیک از **Initiator** ها مجاز به دسترسی به کدام **Target** ها هستند یا نیستند.
- **Initiator** ها را بر اساس یکی از موارد زیر، تعریف می کنیم:
  - **DNS Name**
  - **IQN**
  - **IP Address**

iSNS Server :

از طرف دیگر، وقتی تعداد **Initiator** ها و **Target** ها زیاد باشد، این تعریف های **Permission** درون **iSCSI Target**، کاری زمانگیر خواهد بود؛ پس درون **iSCSI Target** قابلیتی را راه اندازی می کنیم، به نام **iSNS** ، که :

- بر اساس **DNS Name** کار می کند.
- دارای یک **Database** است، جهت ذخیره ی **Target** ها و **Initiator** ها.

قابلیت MPIO :

جهت حفظ یا افزایش سرعت در زمان استفاده از یک Storage، می توان یک کارت شبکه ی دیگر را به Storage اضافه کرد و علاوه بر اتصال قبلی به شبکه، یک اتصال دوم نیز برقرار خواهد شد.

سپس قابلیت MPIO را بر روی آن Storage فعال می کنیم، تا هردو مسیر را به صورت یک مسیر یگانه درنظر بگیرد، در غیراینصورت، هردو مسیر بصورت جدا از هم بررسی می کند.

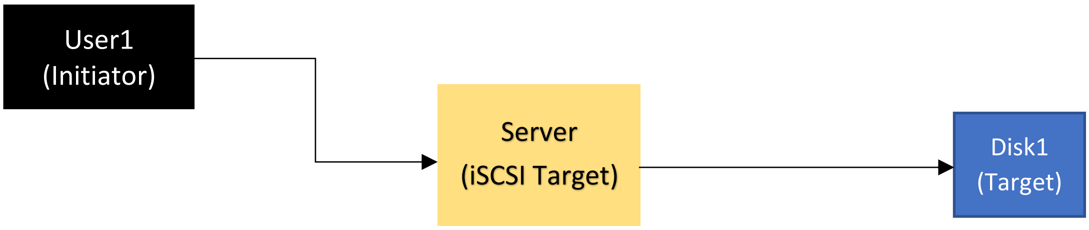
از طریف دیگر، اگر یکی از مسیرها از کار بیفتد، مسیر دیگر، کار را پیش خواهد برد.

نکته: اتصال Storage توسط این دو کارت شبکه به شبکه را می توان توسط اتصال به دو Switch مجزا انجام داد، که باید هردو Switch در همان شبکه باشند.

برای راه اندازی یا فعال سازی آن در Windows Server:

- **پس از راه اندازی تنظیمات iSCSI Server، از منوی Tools گزینه ی MPIO را می زنیم.**
- **حال باید فایل های Driver سخت افزارهای متصل به سیستم را توسط DVD یا به هرشکلی متصل کنیم و در تب DSM Install فایل INF. آن را وارد می کنیم.**
- **در تب Discover Multi-Paths، آن سخت افزار را Add می کنیم.**

:Implementation of iSCSI Target



1. از طریق Add Roles and Features نقش iSCSI Target را نصب می کنیم.

- در تب Roles، وارد File and Storage Services شده و از زیرمجموعه های File and iSCSI Services گزینه ی
- iSCSI Target Server را انتخاب و در تب Features گزینه ی Data Center Bridging و iSNS Server Service و Multipath I/O را انتخاب و نصب می کنیم.
- حال اگر به Server Manager و گزینه ی File and Storage Services برویم، می بینیم که گزینه ی iSCSI اضافه شده است.

2. یک virtual Disk ایجاد و یک Target را به آن متصل می کنیم.

- در همان تب iSCSI، از طریق گزینه ی TASK، گزینه ی New iSCSI Virtual Disk را می زنیم.
- حال باید دیسک هایی مجازی را درون دیسک یا دیسک های فیزیکی متصل به Server، برای این iSCSI Server تعیین کنیم.
- یکی از درایوها را انتخاب کرده و next و یک نام درج کرده و سپس یک حجم را به صورت dynamic یا Fixed تعیین می کنیم.
- هماطور که می بینیم یک iSCASI جدید ایجاد شده که خودکار به این Vdisk ایجاد شده، متصل می شود.
  (به هر iSCSI Target می توان چند Disk را متصل کرد.)
- یک نام برای Target ایجاد می کنیم.
- در تب Access Server، کامپیوترها یا همان Initiator ها را معین می کنیم، پس دکمه ی Add را می زنیم.
  - یا از طریق Query initiator computer می توان از طریق Active Directory به سادگی، PC ها را Add کرد.
  - یا از طریق گزینه ی پایین، و یکی از مشخصه های Type، کامپیوترها را اضافه می کنیم.

نکته: به جهت اینکه این ثبت به عنوان Initiator بطوردائمی خواهد بود، بهتر است که توسط DNS Name یا IQN سیستم ها را معرفی کنیم، و نه توسط IP Address .

❖ پیدا کردن نام IQN :

✓ در سیستمی که به عنوان Initiator تعیین خواهد شد و یا تعیین شده است، در Start درج می کنیم «initiator» و iSCSI initiator را باز می کنیم.

نکته: اگر با خطایی مواجه شدید، باید کنسول Services را باز کرده و گزینه ی microsoft iSCSI Initiator Service را به حالت Automatic در آورده و Start می کنیم.

✓ وارد تب Configuration شده و نام IQN را خواهید دید، که می توان توسط این نام، این سیستم را برای یک iSCSI Target به عنوان initiator تعریف کرد. البته می توان توسط دکمه ی change این نام را تغییر داد که یکبار restart ضروری خواهد بود.

نکته: در حقیقت هر Target هم، یک IQN خواهد داشت.

- در تب Enable Authentication می توان User و Password هایی را برای ورود این Initiator های معرفی شده، تعیین کرد.
- و پس از پایان ایجاد، Target IQN را در کادر پایین خواهید دید.

3. حال دیسک ایجاد شده را به سیستم Initiator ، متصل می کنیم.

- در سیستم Initiator، ابزار iSCSI initiator را باز کرده و در تب Targets و در نوار Target، آدرس IP مربوط به Target را درج کرده و دکمه ی Quick Connect را زده و Done!
- در پایین همین تب، هم می توان متصل و یا قطع شد و هم تنظیمات این اتصال را مشاهده کرد.
- اگر در مراحل تعریف Target برای Disk، رمزعبور CHAP هم تعیین کرده بوده باشیم، در iSCSI Initiator باید در تب Targets آن Target را انتخاب کرده و Connect را زده و در پنجره ی باز شده، دکمه ی Advanced را زده و سپس گزینه ی Enable CHAP log on را فعال کرده و پایین همان تب، User و Password تعیین شده را وارد کنیم و OK.

4. سیستم Initiator را به Target موردنظر، متصل می کنیم.

- حال که در سیستم Initiator و در ابزار iSCSI initiator اتصال برقرار شده است، وارد Diskmanagement می شویم و Target Disk را خواهیم دید، پس آن را Config می کنیم.
- سپس دوباره وارد iSCSI initiator شده و به تب Volumes and Devices رفته و Auto Configure را می زنیم.

LUN (Logical Unit Number):

هر LUN به یک بخش منطقی از فضای ذخیره سازی اشاره می کند.

این بخش می تواند تنها بخشی از یک Disk و یا کل یک Disk و یا فضای کل دو یا چند Disk باشد.

این Disk ها می توانند در Enclosure مربوط به SAN Storage قرار داشته باشند.

نکته: اگر بخواهیم Disk های بیشتری ایجاد و متصل کنیم، کافی ست در همان تب iSCSI، و در کادر بالا (virtual Disks) کلیک راست کرده و New iSCSI Virtual Disk را بزنیم. می توان Disk های جدید را نیز برای همان Target Name قبلی ایجاد کرد که در نتیجه LUN های آنها ترتیبی افزایش می یابد، اما در غیراینصورت، هربار شماره ی LUN ها، مدام از ابتدا شروع خواهد شد.

- برای مشاهده ی LUN های هر DISK، کافی ست در کادر بالای تب iSCSI، بر روی آن کلیک راست کرده و Properties را بزنیم.

5. Initiator را به iSNS متصل می کنیم.

- در سیستم Initiator وارد iSCSI Initiator شده و در تب Discovery و در پایین، دکمه ی Add Server را زده و IP یا Name مربوط به Server را وارد می کنیم و OK!
- برای اطمینان از ثبت شدن Initiator در Server، به Server بازگشته و از منوی Tools گزینه ی iSNS Server را می زنیم و می بینیم.
- وارد PowerShell شده و توسط دستور زیر یک کلاس با مشخصات زیر ایجاد می کنیم:

```
Set-WmiInstance -Namespace root\wmi -Class WT_iSNSServer -Arguments @{ServerName="wds.payamavar.local"}
```

- حال اگر دوباره به کنسول iSNS Server برویم، می بینیم که Target های مربوط به iSCSI را اضافه کرده است.
- اما یک Target اضافی که نامش به pseudo-target ختم می شود، نیز وجود دارد.
- اگر روی هریک از Target ها دابل کلیک کنیم، مشخصات آن را خواهیم دید.
- برای حذف آن Target اضافی، به تب Discovery Domain رفته و از منوی بالا، گزینه ی Default DD را انتخاب کرده و Target Name اضافی را انتخاب و Remove می کنیم و OK!
- در حقیقت، اگر از همان ابتدا، در iSCSI Initiator مربوط به سیستم Initiator، فقط iSNS Server را در تب Discovery تنظیم می کردیم، و در تب Targets، دکمه ی refresh را می زدیم، به طور خودکار Target های موجود در Server را اضافه می کرد.
- حال هر Target جدیدی که در Server ایجاد شود، فقط کافی که در iSCSI Initiator مربوط به Client ها، یکبار refresh را بزنیم.
- برای مشاهده ی تنظیمات iSNS Server و یا حذف آن، از دستورات زیر کمک می گیریم:

```
Get-WmiObject -Namespace root\wmi -Class WT_iSNSServer
Get-WmiObject -Namespace root\wmi -Class WT_iSNSServer -Filter "ServerName='wds.payamavar.local' " | Remove-WmiObject
```

: Storage Replica

Storage Replica یا به اختصار SR، یکی از Feature های Windows Server است که جهت فرآیندهای زیر بکار می رود:

- Disaster recovery : بازیابی اطلاعات پس از یک رخداد مخرب، که دستگاه ها کاملاً از بین بروند. شامل دو مشخصه است:
  - RPO (Recovery Point Objective): سطح پذیرش و تحمل Data loss را مشخص می کند.
  - RTO (Recovery Time Objective): مدت زمان قابل تحمل برای دوام شبکه ی سازمان را با از دست رفتن داده ها مشخص می کند.
- Disaster Preparedness : آمادگی در برابر حذف یا ازبین رفتن ناخواسته ی اطلاعات.

برخی قابلیت های Replica:

- بر اساس Volume ها کار می کند (Volume Base).
- انتقال داده ها را به صورت Block انجام می دهد. (Block Base)

تکنولوژی Storage Replica به دو شکل می تواند کار کند:

- Replication همزمان (Synchronous):

داده ها بصورت همزمان، روی دو مقصد (Volume) نوشته می شوند.

سپس برای برنامه ی تولیدکننده ی این داده ها، پیام موفقیت آمیز بودن عمل I/O ارسال می شود.

زمانی از این نوع Replication استفاده می شود که اتصال پرسرعتی بین Volume ها وجود داشته باشد و داده ها بتوانند به سرعت بین ولومها Mirror شوند.

این Replication تضمین می کند که در زمان وقوع یک حادثه، هیچ داده ای از بین نمی رود (Data loss را به صفر می رساند)، پس قابلیت Failover برقرار می باشد.

مقداری سرعت Application ها را کاهش می دهد.

از این روش، معمولاً بین Server های دو شعبه و یا دو Rack استفاده می شود.

- Replication غیرهمزمان (Asynchronous):

داده ها ابتدا روی یک مقصد (Volume) نوشته می شوند و بلافاصله پیام موفقیت آمیز بودن عمل I/O برای برنامه ی تولیدکننده ی آن داده ها ارسال می شود.

سپس همان داده ها با مقصد دوم (یک Volume دیگر) Replicate می شوند.

زمانی از این نوع Replication استفاده می شود که بین Volume ها یک اتصال کُند، مثل WAN Link برقرار باشد.

یعنی زمانی که Volume ها در Site های فیزیکی متفاوتی قرار داشته باشند که درنتیجه سرعت replicate پایین باشد.

با توجه به اینکه یک فاصله زمانی بین نوشته شدن داده ها در Volume اول، و انجام replication در Volume دوم وجود دارد، این احتمال وجود دارد که در طی این فاصله ی زمانی، خطا یا حادثه ای رخ داده و باعث نابودی داده ها شود!

پس این روش Failover را تضمین نمی کند.

از این روش، معمولاً بین Server های دو شهر و یا دو کشور استفاده می شود.

بر اساس Storage Replica، قابلیت محافظت همزمان از داده‌ها درکشورها، شهرها، Campus ها، ساختمان‌ها، طبقات و Rack های مختلف، و عدم از دست رفتن داده‌ها تضمین می شوند.

✓ Storage Replica می تواند به عنوان جایگزینی مناسب برای سیستم‌های File Replication کنونی، مثل DFS Replication که File Level بوده و به عنوان راهکار سطح پایین Disaster Recovery شناخته می‌شود، استفاده گردد.

روش های پیاده سازی Storage Replica :

1. Server-to-Server :

- بین دو Server مبدأ و مقصد، یک رابطه ی partnership ایجاد می شود.
- در هریک از Server های مبدأ و مقصد، حداقل به دو Volume نیاز دارد، یکی برای Log ها و یکی برای Replication.
- بصورت default، نوع ارتباط از نوع synchronous خواهد بود.
- این SR به صورت دستی، بر روی Server انجام می شود.
- عملیات Failover (بازیابی اطلاعات از Server دوم، در صورت بروز حادثه) به صورت دستی یا manual انجام می شود.
- تا قبل از عملیات Failover، به اطلاعات replicate شده بر روی Server دوم، دسترسی نخواهیم داشت.

2. Cluster-to-Cluster :

- در هریک از شبکه های مبدأ و مقصد، یک Cluster از Storage ها ایجاد شده و میان آنها partnership ایجاد می شود.
- عملیات Failover به صورت دستی یا manual انجام می شود.

3. Stretch Cluster :

- همه ی Storage های مبدأ و مقصد، در یک Cluster قرار می گیرند.
- عملیات Failover به صورت automatic انجام می شود.

4. Server-to-Self :

- در هریک از Server های مبدأ و مقصد، حداقل به چهار Volume نیاز دارد:
دوعدد برای Source Log و Destination Log و دوعدد برای Source Replication و Destination Replication.
- پیشنهاد می شود که Log Volume ها بر روی حافظه های SSD قرار داشته باشند.

:Implementation of Storage Replica



- باید تمام این Volume ها دارای حجمی یکسان و همچنین Partition Table از نوع GPT باشند.
- در هریک از Server ها، نام یکی از Volume ها را Log و دیگری را Replica قرار می دهیم.
- Firewall هردو Server باید طوری تنظیم شود که برای پورتهای زیر، اجازه ی ترافیک داده شود:
  - پروتکلICMP
  - پروتکل SMB : 445 و 5445
  - web Service Management : 5985

1. در هردو Server، سرویس یا Role های SR و FileServer را نصب می کنیم:

- یا به صورت تکی:

```
Install-WindowsFeature -Name storage-Replica,FS-Fileserver -IncludeManagementTools -Restart
```

- یا هردو باهم:

```
Invoke-Command -ComputerName DC1,DC2 -ScriptBlock{
Install-WindowsFeature -Name storage-Replica,FS-Fileserver -IncludeManagementTools -Restart}
```

2. SRTopology را تست می کنیم.

در طی این تست، بررسی می شود که پیش نیازهای لازم برای انجام SR میان این دو Server، وجود دارند یا خیر.
نتیجه ی این تست، در یک فایل HTML ایجاد می شود:

```
Test-SRTopology -SourceComputerName DC1 -SourceVolumeName G -SourceLogVolumeName F: -DestinationComputerName DC2 -DestinationVolumeName G: -DestinationLogVolumeName E: -DurationInMinutes 1 -ResultPath c:\Folder1 -IgnorePerfTests
```

- Sourcecomputername: نام سرور مبدا
- Sourcevolumename: ولوم داده ها در مبدا
- Sourcelogvolumename: ولوم log در مبدا
- Destinationcomputername: نام سرور مقصد
- Destinationvolumename: نام ولوم داده ها در مقصد
- Destinationlogvolumename: نام ولوم log در مقصد
- Durationminites: زمانی دلخواه جهت انجام تست
- Resultpath: مکان قرار دادن فایل html مربوط به گزارش پاسخ تست
- IgnorePerfTest: عملیات تست و بررسی توسط نمایش یک نمودار را قطع می کند.

در فایل نتیجه ی HTML می بینیم که دست کم 20 تست را انجام داده که احتمال وجود تعدادی Warning و Messeage وجود دارد، اما نباید Error وجود داشته باشد.

3. Partnership را تست می کنیم.

```
New-SRPartnership -SourceComputerName DC1 -SourceRGName MyGroup1 -SourceVolumeName G: -SourceLogVolumeName F: -DestinationComputerName DC2 -DestinationRGName MyGroup2 -DestinationVolumeName G: -DestinationLogVolumeName E: -ReplicationMode Synchronous
```

در حقیقت، RGName یک نام دلخواه است برای یک گروه به نام Replication Group.

پس از ایجاد این Partnership، اولین اتفاقی که می افتد، از دسترس خارج شدن، Replicate Volume مربوط به Server مقصد است.

برای مشاهده ی وضعیت ReplicationGroup درج می کنیم:

```
Get-SRGroup
```

و برای مشاهده ی تنظیمات مربوط به Replica در ReplicationGroup درج می کنیم:

```
(Get-SRGroup).Replicas
```

Restore Storage Replica :

حال اگر Volume مربوط به Replication در Server اول دچار مشکل شده و بخواهیم، داده ها را از Volume به همین نام، در Server دوم بازیابی کنیم، در Server اول دستور زیر را وارد می کنیم:

- Partnership را برعکس یا reverse می کنیم.

```
Set-SRPartnership -NewSourceComputerName DC2 -SourceRGName MyGroup2 -DestinationComputerName DC1 -DestinationRGName MyGroup1
```

حال همان Volume در DC2 باز شده و در DC1 بسته می شود.

Delete the Storage Replica :

1. Partnership را حذف می کنیم.

```
Get-SRPartnership | Remove-SRPartnership
```

2. با وارد کردن دستور زیر در هر دو Server، SRGroup را در هردوی آنها حذف می کنیم.

```
Invoke-Command -ComputerName WDS,DC1 -ScriptBlock{Get-SRGroup | Remove-SRGroup}
```

Data Deduplication :

- این تکنولوژی روشی است که با عدم ذخیره ی داده های تکراری، نیازهای ذخیره‌سازی را کاهش می دهد.
- علاوه بر کاهش نیاز به فضای ذخیره‌سازی، مقدار Byte های ارسالی در هنگام انتقال Data در شبکه نیز کاهش می‌یابند.
- این روش با نام‌های دیگری مثل Intelligent Compression و SIS (Single-Instance Storage) نیز شناخته می‌شود.

در این تکنیک طی یک پروسه ی تحلیلی، تنها یک نمونه از داده در رسانه ی ذخیره‌سازی، ذخیره می‌شود و داده ی تکراری توسط یک اشاره گر (Pointer) ارجاع داده می شود.
مثلا یک ایمیل معمولی ممکن است صد نمونه از یک فایل پیوست یک مگابایتی داشته باشد.
برای Backup گیری از آن، باید تمامی صد نمونه ذخیره شوند که به فضای ذخیره‌سازی ۱۰۰ مگابایتی نیاز دارد.
اما با استفاده از Dedupe، تنها یک نمونه از این فایل ذخیره می‌شود و نمونه‌های بعدی به همان یک نسخه ی ذخیره شده، ارجاع داده می‌شوند. همانطور که می بینید، هر صد مگابایت مورد نیاز، می‌تواند به تنها یک مگابایت کاهش یابد.

- نیاز به Disk های ذخیره سازی را کاهش می دهد.
- نیاز به Backup گیری را کاهش می دهد.
- در موارد Replication و Disaster Recovery نیاز کمتری به Bandwidth خواهد بود.

عملیات Deduplication شامل چهار Job می باشد:

- Optimization :
  - عملیات اصلی Duplicating را انجام داده و فایل های تکراری را جدا می کند.
  - بطورپیشفرض، هریک ساعت اجرا می شود.
- Garbage Collection :
  - فضاهای خالی ناشی از deduplication ها را بازسازی کرده و به سیستم باز می گرداند.
  - بطورپیشفرض، هریک هفته اجرا می شود.
- Integrity Scrubbing :
  - در صورت وجود Data Corruption (داده ی خراب) آن را شناسایی و حدالامکان ترمیم می کند.
  - بطورپیشفرض، هریک هفته اجرا می شود.
- Unoptimization :
  - در صورت اجرا، تمام تنظیمات Deduplication را قطع و به حالت اول باز می گرداند.

در سه حالت می توان از Deduplication استفاده کرد:

- Default : موارد کلی و عمومی مثل File Server ها
- Hyper-V : دیسک های مجازی و زیرساخت دسکتاپهای مجازی (VDI)
- Backup : برای نرم افزارهای پشتیبان گیری

صرفه‌جویی معمول در فضا	محتوا
30 تا 50 درصد	فایل‌های Office ، عکس‌ها، موسیقی، فایل ویدیویی و سایر موارد
70 تا 80 درصد	فایل‌های باینری مربوط به نرم‌افزارها، فایل‌های Cab ، نمادها و سایر موارد
80 تا 95 درصد	فایل‌های ISO ، فایل‌های مربوط به هارد دیسکِ مجازی و غیره
50 تا 60 درصد	شامل تمام موارد فوق

: Implementation of Data Deduplication

به عنوان مثال، در یکی از Partition ها، چند فایل iso. و در یک Partition دیگر، چند فایل vhdx. قرار می دهیم.

- وارد Add Roles and Features شده و در تب Server Roles در زیرمجموعه های File and iSCSI Services گزینه ی Data Deduplication را انتخاب و نصب می کنیم.

و یا:

```
Install-WindowsFeature -Name FS-Data-Deduplication
```

- می توانیم توسط دستور زیر که همراه با نام Partition موردنظر می آید، یک ارزیابی از حجم فایل های یک Partition، پس از Deduplicate شدن، را بدست بیاوریم:

```
ddpeval F:
```

حجم کنونی و حجم پس از عملیات را در گزینه های Evaluated folder size و optimized files Size خواهیم دید.

- در Server Manager وارد File and Storage شده و در تب Volumes، بر روی هریک از Partition های موردنظر، کلیک راست کرده و Configure Data Deduplication را می زنیم. (مثلاً Partition شامل فایل های ISO)
- برای Data Deduplication گزینه ی General purpose file Server را می زنیم.

و یا در PowerShell:

```
Enable-DedupVolume -Volume F: -UsageType Default
```

- البته اگر فایل های VHDx درون Partition می بودند، باید مقدار UsageType را برابر با HyperV قرار می دادیم.
- و توسط دستور زیر، می توان مشخصات Deduplication این Volume را مشاهده کرد:

```
Get-DedupVolume -Volume F: | Format-List *
```

- با درج یک شماره برای deduplicate files older than، تعیین می کنیم که فایل هایی که قدیمی تر از این تعداد روز هستند، را Deduplicate کند.

و یا برای تغییر این عدد، در PowerShell :

```
Set-DedupVolume -Volume F: -minimumfileagedays 1
```

- در کادر پایین و از طریق دکمه ی Add، می توانیم فایل هایی که نمی خواهیم Deduplicate شوند را اضافه کنیم.
- از طریق دکمه ی Set Deduplication Schedule می توانیم زمانبندی های پیشفرض را تغییر دهیم:
- برای اینکه این عملیات را با تمام قدرت و در زمان هایی دلخواه انجام دهد، گزینه ی Enable throughput را فعال و زمانبندی را مشخص می کنیم.
- توسط کادر پایینی، می توان یک زمانبندی دیگر هم تعریف کرد.
- هردوپنجره را OK کرده و خروج!

- برای اجرای دستی و یا حذف دستی Deduplication ایجاد شده، در PowerShell درج می کنیم:

```
Start-DedupJob -Type Optimization -Volume F: -Priority High -Memory 100 -Cores 100
Start-DedupJob -Type Unoptimization -Volume F: -Priority High -Memory 100 -Cores 100
```

- مقادیر 100 برای Memory و Cores ، بر حسب درصد هستند، که می توان آنها را کمتر کرد تا همه ی قدرت سیستم را اشغال نکنند.
- توسط دستور زیر می توان میزان پیشرفت این Deduplication را monitor یا نظارت کرد:

```
Get-DedupJob
```

- در پایان توسط دستور زیر می توان تأثیرات Deduplication بر روی Partition را مشاهده کرد:

```
Get-DedupStatus | Format-List *
```

- برای مشاهده و تغییر زمانبندی های موجود برای Job ها:

```
Get-DedupSchedule
Set-DedupSchedule -Name weeklyscrubbing -Start 04:00 -Enabled $true
```

DFS (Distributed File System):

در شبکه ی شرکت های بزرگ، Windows Server 2016 ابزاری به نام DFS را در اختیار مدیر شبکه می گذارد.
این ابزار یک ساختار منطقی و منسجم از فولدر هایی ست که هریک از Server ها در شبکه share کرده اند.
در حقیقت آنچیزی که همه ی کاربرها می بینند، یک پوشه ی Share شده ی حاوی یک سری فایل و پوشه است، اما در واقعیت آن پوشه ها و فایل ها، می توانند بر روی چندین Server متفاوت قرار داشته باشند.

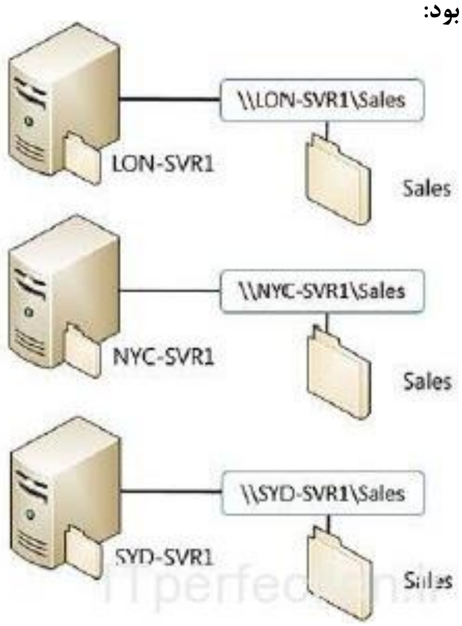
DFS این امکان را به کاربران می دهد که برای دسترسی به همه ی پوشه های Share شده در شبکه، از یک نام واحد استفاده کنند.
توسط DFS، دستیابی به Folder های share شده، دیگر وابسته به دانستن آدرس دقیق UNC پوشه ها نیست و مدیران شبکه می توانند به راحتی File Server را تغییر دهند و یا مدارک و Folder ها را بدون اطلاع کاربران، از روی یک Server به یک Server دیگر جابجا نمایند.

در حقیقت DFS دارای یک پوشه ی Share شده (ریشه) با یک نام ثابت است که درون آن، لینک های همه ی پوشه های Share شده در شبکه وجود دارند و کاربران از طریق همین Folder ثابت (ریشه) می توانند به همه ی Folder های شبکه دسترسی داشته باشند.
در صورت عوض شدن مسیر یک Folder، تنها کاری که مدیر شبکه باید انجام دهد، این است که لینک مربوط به آن Folder ریشه را اصلاح کند.
پس DFS ما را قادر می سازد که File Server خود را روی چندین Server ایجاد کنیم.
کاربر نهایی نیازی به دانستن اسم آن Server ها ندارد بلکه با یک کلِ واحد سروکار دارد.
کاربران پس از اتصال به ریشه ی DFS، به تمام زیرمجموعه های ریشه، فارغ از محل Server آن منابع، می توانند دسترسی داشته باشند.
ساختار DFS تشکیل شده است از درختی با یک ریشه و تعدادی لینک.
هر ریشه می تواند دارای چندین لینک در زیرمجموعه ی خودش باشد که هر لینک به یک Folder اشتراکی مرتبط است.این Folder های اشتراکی، از نظر فیزیکی ممکن است روی Server های مختلفی باشند.

به منظور پیکربندی DFS باید با اجزای آن آشنا باشید:

- NameSpace : نامی ست که برای کاربران شبکه قابل دیدن است و کاربران از این نام برای دسترسی به فولدر های File Server استفاده می کنند.

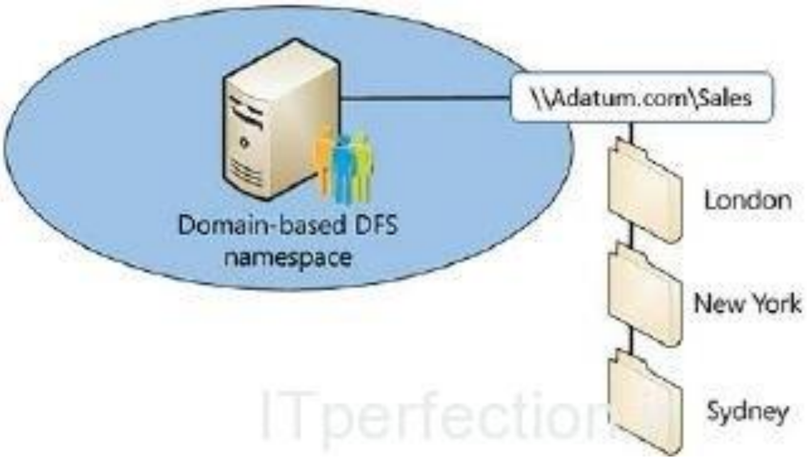
در حقیقت NameSpace شروع سلسله مراتب DFS است و به شکل یک Folder ثابت، در شبکه Share شده است که درون آن لینکهایی قرار دارند که ما را به Folder های Share شده ی File Server هدایت می کنند.
پس اگر DFS وجود نداشته باشد، این Shared Folder ها در شبکه به صورت زیر خواهند بود:



همانطور که می بینید، برای دسترسی به Shared Folder های هر Server باید نام آن Server را نیز بدانیم.
شبکه ی روبرو، دارای سه عدد Server در سه مکان فیزیکی مختلف می باشد.
هر کدام از File Server ها برای شعبه ی خود، فولدری را به نام Sales به اشتراک گذاشته است.

در سیستم DFS کاربر اصلاً متوجه نمی شود که در حال حاضر به کدام Server متصل شده است. او فقط روی فایل ها کار می کند.

پس در ابتدا باید ریشه ی درخت را تعیین کرد که به آن NameSpace گفته می شود.
در حقیقت ابتدای نام همه ی ریشه ها، نام Domain می آید. مثلاً برای دامین Adatum.com به شکل زیر می شود.



سپس برای هریک از بخش های مشترک در تمام DC ها، یک NameSpace در DFS Server ایجاد می کنیم.مثلاً:
\\Adatum.com\Purchase
\\Adatum.com\Accountig
و برای هریک از این NameSpace ها، آدرس مربوط به پوشه ی موردنظرشان را در تک تک DC های شهرهای دیگر، Add می کنیم.
برای اضافه کردنِ Link پوشه های Share شده ی مربوط به DC های دیگر، در کنسول DFS، نیاز به یک Folder جدید درون NameSpace خواهیم داشت که لینکها پراکنده و درهم نشوند!

DFS را می توان به دو شکل پیاده سازی کرد:

- بصورت Domain Base : یک Active Directory Server که عضو Domain است، نقش Name Space را به عهده می گیرد.
- بصورت Stand alone : یک Server که عضو Domain نباشد، اما به شبکه متصل است، نقش NS را می گیرد.

در نتیجه یک Stand alone DFS Server، قابلیت High Availability ندارد، چون اگر از کار بیفتد، یک Name Server دیگر نمی تواند جایگزین آن شود.

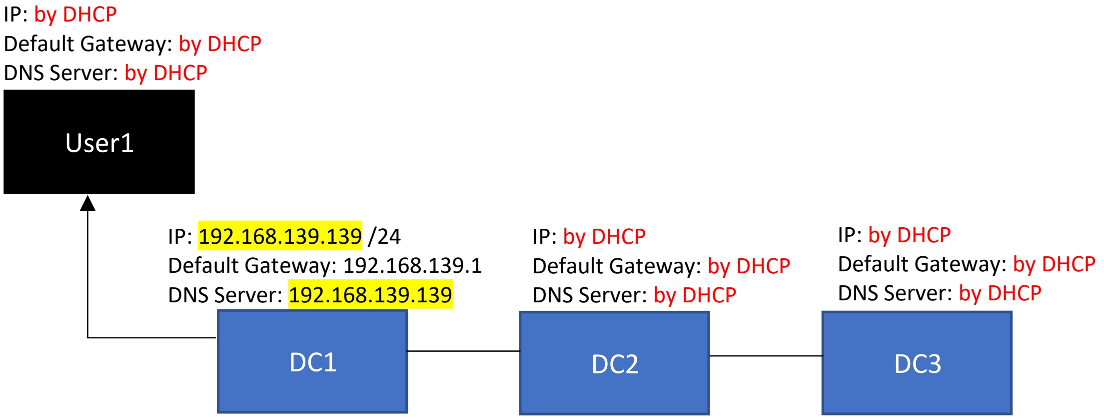
DFS Replication:

- در حقیقت یک Role جدا از DFS NameSpaces است که آن را بر روی DC های دیگر نصب می کنیم.
- این Role، یک کپی از Shared Folder ها می گیرد.که بر طبق سرویس FRS (File Replication Service)، مراقب است که محتویات Folder ها بصورت Sync باقی بمانند.

- اگر فقط دو DFS Server در شبکه داشته باشیم، DFS Replication را بین آنها ایجاد می کنیم، اما اگر تعداد DFS Server هایی که باید اطلاعات را بین خود مبادله کنند، از دو تجاوز کند، بهتر است یک Replication Group ایجاد کنیم.

Implement a DFS :

می خواهیم این قابلیت را ایجاد کنیم که یک پوشه ی مشترک، در تمام هرسه DC زیر ایجاد شود که همیشه به سرعت **Replicate** شود.



1. **ابتدا نقش DFS را بر روی DC ها نصب می کنیم.**

- ابتدا در **DC1** : می توانیم در **Add Roles and Features** وارد شده و نقش **File and Storage Services** و از زیر گزینه هایش، **File and iSCSI Services** و سپس **DFS NameSpaces** را نصب کنیم.
- و یا اینکه در **PowerShell** این **DC** درج کنیم:

```
Install-WindowsFeature fs-dfs-namespace -IncludeAllSubFeature -IncludeManagementTools
```

- حال قابلیت **DFS-Replication** را بر روی **DC2** و **DC3** نصب کنیم:

```
Icm -computerName DC2,DC3 -Command {Install-WindowsFeature fs-dfs-Replication -IncludeAllSubFeature
-IncludeManagementTools}
```

- به این صورت ریشه ی این **DFS** در **DC1** قرار می گیرد که قادر به مدیریت کامل آن می باشد و **DC** های یک و دو، فقط قابلیت دسترسی و ایجاد تغییر در محتوا را خواهند داشت.

2. **در هریک از DC های یک و دو، یک پوشه را به دلخواه Share می کنیم.**
3. **Name Space را ایجاد می کنیم.**

- وارد **DC1** شده و در **Server Manager** از منوی **Tools** گزینه ی **DFS Management** را می زنیم تا کنسول آن باز شود.
- در کادر سمت چپ، بر روی **NameSpace** کلیک راست کرده و **New NameSpaces** را می زنیم.
- از طریق دکمه ی **Browse**، سروری که قصد داریم تبدیل به **NameSpace Server** شود را انتخاب می کنیم.
- یک نام برای آن انتخاب کرده و در قسمت **Setting**، می توانیم گزینه ی All Users have Read and Write Perm را بزنیم.
- **Domain-based namespace** را انتخاب کرده و **Create** و تمام!

4. **Shared Folder ها و replication Group را وارد و ایجاد می کنیم.**

- بر روی **Root NameSpace** ایجاد شده، کلیک راست کرده و **New Folder** را می زنیم.
- یک نام درج کرده و دکمه ی **Add** را زده و در نوار **Path to folder target**، ابتدا باید **Server** موردنظر را فراخوانی کنیم و سپس توسط دکمه ی **Browse** پوشه ی **Share** شده ی آن را وارد کنیم. پس در این نوار برای هر **Server** بصورت زیر درج می کنیم:

\\\\نام سرور

- سپس می پرسد آیا می خواهید یک **Replication Group** هم بین این دو پوشه ایجاد شود؟ پس **yes**
- **Name** ها را بخاطر سپرده و **Next** کرده و برای **Primary member** یکی از آن دو را انتخاب می کنیم.
- با توجه به اینکه در هردوی آنها، نقش **DFS-Replication** نصب شده است، فرقی نمی کند کدام را انتخاب کنیم. (مثلاً DC2)
- بهترین و کارآمدترین گزینه **Full mesh** خواهد بود.
- سپس زمان و میزان پهنای باند موقع **Replication** را انتخاب می کنیم.(مثلاً **Full** را می زنیم.) و تمام!

5. DFS و Replication Group را تست می کنیم.

- در حقیقت هرتغییری در پوشه ی Share شده ی درون هریک از DC ها ایجاد شود، درون Server های دیگر نیز اعمال می شود.
- کافی ست در یکی از Server ها، هریک از پوشه های Share شده ی مربوط به هریک از Server ها را باز کنیم.سپس در یک پنجره ی دیگر، آدرس زیر را وارد کنیم:

\\Domain آدرس\نام Root NameSpace
\\payamavar.local\my RootNS

6. جهت ایجاد High Availability یک NameSpace جانشین اضافه می کنیم.

- فرض کنید، سیستم NameSpace موجود در شبکه که در اینجا DC1 است، از کار بیفتد یا دچار اشکال در اتصال به شبکه شود، در نتیجه نیاز به یک NameSpace دیگر خواهیم داشت تا مانع از دست رفتن دسترسی به داده های Share شده شویم.
- پس در سیستم NameServer (DC1) هم نقش Replication را نصب می کنیم:

```
Install-WindowsFeature fs-dfs-namespace -IncludeAllSubFeature -IncludeManagementTools
```

- سپس در سرور موردنظر دیگر (مثلاً DC3) هم نقش NameSpace را نصب می کنیم:

```
Install-WindowsFeature fs-dfs-namespace -IncludeAllSubFeature -IncludeManagementTools
```

- سپس در کنسول DFS Management موجود در DC1 بر روی آبجکت Root مربوط به NameSpace کلیک راست کرده و Add Namespace Server را زده و نام NameSpace مربوط به DC3 را وارد کرده و بر روی Edit Setting زده و گزینه ی All Users have Read and Write Perm.را می زنیم و OK!
- حال اگر این Root NameSpace را انتخاب کرده و وارد تب NameSpace Server شوید، می بینید که اضافه شده است.
- حال یکبار در DC3 وارد DFS Management شده و این گزینه ها را چک کنید.
- برای اطمینان از کارآیی این NameSpace Server جدید، DC1 را از شبکه جدا می کنیم و در یک File Explorer درون DC3 آدرس NameSpace ریشه را وارد می کنیم؛ که باید وارد شود.مثلاً:

\\payamavar.local\my RootNS

پس در حقیقت:

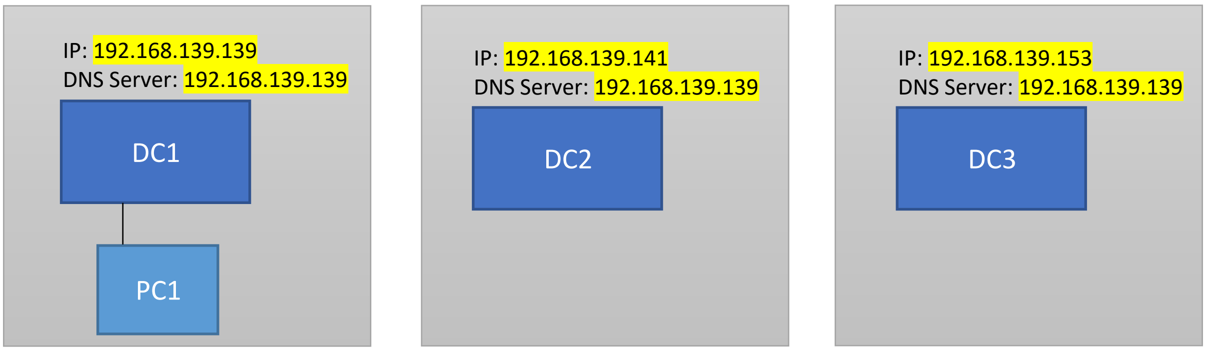
- برای قابلیت High Availability باید حداقل دو DFS server در Domain خود قرار دهیم که اطلاعات Namespace ها و لینک ها را بین خود replicate کنند.
- در این حالت File Server ها دارای خاصیت failover می باشند.
- یعنی اگر منبع اولیه اطلاعات غیر قابل دسترس شود، DFS کاربر را به نسخه ی دوم از اطلاعات هدایت می کند.
- DFS ابتدا درخواست ها را به Local DFS می فرستد، اما اگر پاسخی دریافت نکرد، آنگاه درخواست را به سرور پشتیبان هدایت می کند.

نکته: وقتی پوشه ی موجود در NameSpace در یکی از شعبه های متصل به DFS نمی تواند replicate شود، باید size of staging area را تغییر دهیم که توسط دستور زیر انجام می شود:

```
set-DfsrMembership
```

: DFS Server for Sites

فرض کنید شبکه ی شما دارای سه سایت به صورت زیر است.(البته با رنج IP های مناسب)
و قصد داریم قابلیت DFS را برای همه ی آنها راه اندازی کنیم، با این تفاوت که فایل های هر سایت، فقط برای اعضای آن سایت قابل دسترسی کامل باشند.



برای اینکه به سیستم های دیگر بفهمانیم که هریک از DC ها درون یک سایت متفاوت قرار دارد، باید Prefix مربوط به IP آن DC را برابر با 32 قرار دهیم، طوری که انگار تمام بیت های آن برای NET ID اشغال شده اند.

1. **تنظیمات Site ها را انجام می دهیم.**
   - به کنسول **AD Sites and Services** رفته و در کادر سمت چپ، بر روی پوشه ی **Sites** کلیک راست کرده و **New Site** را می زنیم.
   - یک نام برای آن درج می کنیم (مثلاً **Site1**) و در کادر پایین گزینه ی سایت درج شده را انتخاب و **OK** می کنیم.
   - دقیقاً به همین شکل عمل کرده و دو سایت دیگر **Site2** و **Site3** را ایجاد می کنیم.
2. **آدرس های DC ها و Client ها را برای Site ها تعریف می کنیم.(در اینجا بطور آزمایشگاهی!)**
   - بر روی پوشه ی **Subnets** کلیک راست کرده و **new Subnet** را می زنیم.
   - برای **prefix** آدرس **IP** مربوط به **DC1** را بصورت **192.168.139.139/32** درج و در کادر پایین **Site1** را انتخاب و **OK** می کنیم.
   - دقیقا به همین شکل، آدرس **prefix** را برای **DC** های دو و سه
   - و دقیقا به همین شکل برای مثلاً یک **Client** برای هریک از **DC** ها اضافه می کنیم.
3. **در هریک از DC ها، یک پوشه را به دلخواه Share می کنیم.**
4. **Name Space را ایجاد می کنیم.**
   - وارد **DC1** شده و در **Server Manager** از منوی **Tools** گزینه ی **DFS Management** را می زنیم تا کنسول آن باز شود.
   - در کادر سمت چپ، بر روی **NameSpace** کلیک راست کرده و **New NameSpaces** را می زنیم.
   - از طریق دکمه ی **Browse**، سروری که قصد داریم تبدیل به **NameSpace Server** شود را انتخاب می کنیم.
   - یک نام برای آن انتخاب کرده و در قسمت **Setting**، می توانیم گزینه ی **All Users have Read and Write Perm** را بزنیم.
   - **Domain-based namespace** را انتخاب کرده و **Create** و تمام!
5. **یک DFS Folder ایجاد می کنیم که replication نداشته باشد.**
   - بر روی **Root NameSpace** ایجاد شده، کلیک راست کرده و **New Folder** را می زنیم.
   - یک نام درج کرده (مثلاً **DFS-S1**) و دکمه ی **Add** را زده و با دکمه ی **Browse** پوشه ی **Share** شده ی روی **DC1** را وارد کنیم.
   - دوباره **Add** را زده و پوشه های **share** شده ی موجود در **Server** های دیگر را نیز وارد می کنیم.
   - سپس می پرسد آیا می خواهید یک **Replication Group** هم بین این دو پوشه ایجاد شود؟ پس **NO**

6. DFS را چک می کنیم.

- در هریک از DC ها یا Client ها، وارد آدرس Domain می شویم: payamavar.local
- وارد پوشه ی NameSpace و سپس پوشه ی DFS Folder می شویم که باید فقط فایلهایی که برای آن Site به اشتراک گذاشته بودیم را ببینیم.
- اگر نشد، باید یکبار سیستم را Restart کنیم تا Cache آن یکبار خالی شده و از نو ارتباط را بررسی کند.
- اما راه حل دیگر برای اینکه این Cache سیستم ها سریع تر و بدون Restart تخلیه شود، این است که در DFS Management وارد properties آبجکت ریشه (یعنی \\payamavar.local\myNameSpace) شده و در تب referrals مقدار Cache du. را کمتر کنیم.

دقیقاً همین گزینه در Properties پوشه های لینک شده نیز وجود دارد.

BranchCache :

این تکنولوژی به کاربران راه دور (مثلاً در شعبه ی دیگر) اجازه می‌دهد به اطلاعات موجود در Server های دفتر مرکزی با سرعتی بسیار بالا دسترسی داشته باشند.

یکی از بزرگ‌ترین مشکلاتی که کاربران راه دور با آن درگیر هستند، اتصال به دفتر مرکزی با کمک لینک‌های WAN کم سرعت و یا ارتباطات S2S VPN است که منجر به مشکلات مختلفی مثل کُندی ارتباط در دسترسی به اطلاعات شده و باعث کاهش بازدهی کسب و کار سازمان می شود.

از مزیت های BranchCache کاهش استفاده از خطوط دیتا و پهنای باند است!

BranchCache داده ها را روی یکی از کامپیوترهای شعبه فرعی cache کرده و به کاربران Remote اجازه می دهد تا با فایل ها در محیطی که دقیقا همانند کامپیوترشان در اداره اصلی است، کار کنند.

به این صورت ترافیک داده ها روی WAN Link ها را کاهش می دهد و سرعت پاسخگویی به نرم افزارهای تحت شبکه را بسیار بالا می برد.

به این صورت که وقتی کاربران یک شعبه، اطلاعاتی را از Datacenter مرکزی (در شعبه اصلی سازمان) دریافت می کنند، یک کپی از این اطلاعات بر روی یکی از کامپیوترهای شبکه داخلی آن شعبه Cache می شود.

درخواستهای بعدی برای آن اطلاعات، از روی نسخه ی Cache شده، پاسخ داده می شوند.

پس کلاینت ها به جای دریافت داده های مورد نیاز خود از روی لینک WAN، ابتدا Cache محلی را چک می کنند.

وقتی تاخیرهای رفت و برگشتی جهت دریافت داده ها از Datacenter مرکزی، بیشتر از حد threshold (80 میلی ثانیه) طول کشید، Branchcache فعال می شود.

این فعال شدن، مراحل زیر را طی می کند:

1. Client بررسی می کند که آیا Datacenter مرکزی، قابلیت Branchcache را ساپورت می کند یا نه؟
2. Client بررسی می کند که آیا تأخیر Send و Receive از مقدار threshold بیشتر شده است یا نه؟
3. Client بررسی می کند که آیا داده های موردنظر، در شبکه ی شعبه ی خودش، Cache شده اند یا نه؟
4. اگر داده ها Cache شده باشند، Client بررسی می کند که آیا آنها Updated هستند یا نه؟
5. اگر داده های موردنظر Cache نشده باشند یا Updated نباشند، داده ها از Datacenter مرکزی دریافت و Cache می شوند.

تکنولوژی BranchCache به دو صورت قابل پیاده‌سازی است:

- **Hosted Cache Mode :**

مخصوص شبکه های Domain است.بر روی Server شبکه نصب می شود و آنرا تبدیل به Hosted Cache Server می کند؛ و مدام اطلاعات دریافتی از Server شعبه ی اصلی را درون آن Cache می کند.

- **Distributed Cache Mode :**

در این حالت باید قابلیت Cache کردن را بر روی تک تک Client ها تعریف کنیم.

در این حالت، اگر یکی از Client ها نیاز به یک فایل از Server اصلی داشته باشد، ابتدا یک Query در سطح شبکه ی شعبه ی خودش به همه ی اعضا ارسال می کند که اگر کسی آنرا قبلاً Cache کرده باشد، برایش ارسال می کند و دیگر نیازی به ارتباط با سرور شعبه ی اصلی نیست.

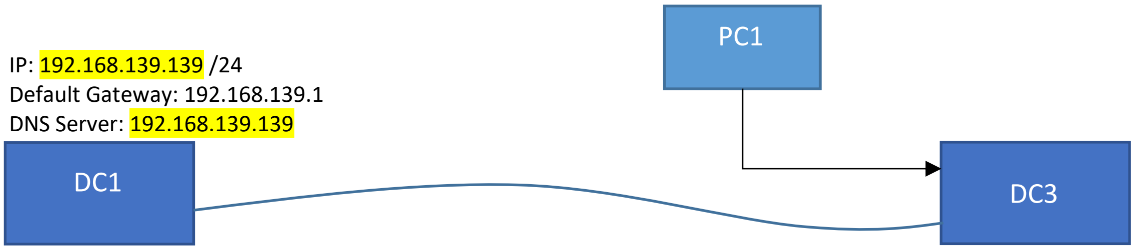
در این حالت، هر بخش از اطلاعات می تواند روی یک Client باشد! یعنی مدیریت جامع و متمرکزی وجود ندارد.

از طرف دیگر، Client ها همیشه روشن نیستند؛ پس به همین جهت با اینکه یک سری داده ها روی کلاینت A ذخیره شده اند، به جهت خاموش بودنِ آن، کلاینت B که به داده ی او نیاز دارد، مجبور به مراجعه به Datacenter مرکزی می شود.

همچنین تمام کامپیوترها در این سناریو باید در یک Subnet باشند.

در هر دو mode از پروتکل HTTP برای انتقال داده ها استفاده می شود که باید در هر دو روش، برای ترافیک ورودی، پورت TCP 80 باز باشد.

Implement a Hosted Cache Mode :



1. یک پوشه در **DC1** را با دسترسی **EveryOne** به اشتراک می گذاریم.

- ابتدا آن را برای **Every One** اشتراکگذاری می کنیم، سپس وارد **Properties** آن شده و در تب **Sharing** وارد **Advanced Sharing** شده و دکمه ی **Caching** را زده و گزینه ی **Enable BranchCache** را فعال کرده و **OK**!
می توانیم درون این پوشه یک سری فایل های گوناگون کپی کنیم.

2. **DC1** را به عنوان **Content Server** پیکربندی می کنیم.

- وارد **Add Roles and Features** شده و:
  - اگر بخواهیم **File Server** شبکه را **Cache** کنیم، (محتوای موردنظر **File** باشد) نقش **File and Storage Services** را و از زیر گزینه هایش، File and iSCSI Services و سپس BranchCache for Network Files را انتخاب کرده و نصب می کنیم.
  - اگر بخواهیم **Web Server** یا **Application Server** شبکه را **Cache** کنیم؛ در تب **Select Features** گزینه ی **BranchCache** را انتخاب و نصب می کنیم.
  - هردوی موارد بالا را نیز می توان نصب و **Cache** کرد.(در اینجا قصد ما **File Server** است.)

3. **DC3** را به عنوان **Hosted Cache Server** پیکربندی می کنیم.

- وارد **Add Roles and Features** شده و فقط در تب **Select Features** گزینه ی **BranchCache** را انتخاب و نصب می کنیم.
- سپس در همین سرور، وارد **PowerShell** شده و برای چک کردن قابلیت **BranchCache** درج می کنیم:

```
Get-BCStatus
```

- بطورطبیعی باید در قسمت HostedCacheServerConfiguration در مقابل HostedCacheServerIsEnabled مقدار **False** درج شده باشد.
- دستور زیر را برای فعالسازی آن وارد می کنیم و دوباره دستور بالا را امتحان می کنیم:

```
Enable-BCHostedServer -RegisterSCP
```

نکته: برای غیرفعال سازی دستور بالا، از دستور زیر استفاده می شود:

```
Disable-BC
```

4. از طریق **Group Policy Management**، قابلیت **BrancheCache** را در شبکه، معرفی و پیکربندی می کنیم.

- در **DC1**، یک **OU** ایجاد می کنیم مثلاً به نام **BR**، که شامل همه ی **Client** های مستقر در شعبه های موردنظر باشد.(طبیعتاً این **OU** خود می تواند دارای **OU** هایی به نام شعبه های متصل باشد.
وارد کنسول **Group Policy Management** شده و یک **GPO** بنام مثلاً **GPO1** ایجاد کرده و آنرا به **BR** لینک می کنیم.
- وارد تنظیمات **GPO1** شده و به مسیر زیر می رویم:

Computer configuration/policies/windows settings/security settings/windows firewall and advanced security

- روی **windows firewall and advanced security** دبل کلیک می کنیم، روی **inbound roles** کلیک می کنیم.
- در قاب سمت راست، کلیک راست کرده و **new rule** را می زنیم.
- در تب اول، گزینه ی **predefined** را و از لیستش، گزینه ی **BranchCache – Content Retrieval (Uses HTTP)** را انتخاب می کنیم.این رول ترافیک ورودی را روی پورت **80** پروتکل **TCP** مجاز می کند.

- تغییر خاصی نیازی نیست.(می توان **Allow the Connection if it’s Secure** را انتخاب کرد.)
- تیک گزینه ی **BranchCache – Content Retrieval** را می زنیم و تمام!
- این عمل را برای هر دو مد **BranchCache** انجام می دهیم.
- در **GP Management** یکی **GPO** دیگر می سازیم به نام **GPO2** و آنرا نیز به **BR** لینک می کنیم.
- وارد تنظیمات **GPO2** شده و به مسیر زیر می رویم:

Computer Configuration > Policies > Administrative Templates > Network >

- ابتدا وارد پوشه ی **Lanman Server** شده و گزینه ی **Hash Publication for BranchCache** را باز کرده و **Enable** کرده و یکی از گزینه های اول یا دوم را در گزینه ی کرکره ایِ کادر پایین انتخاب و **OK** می کنیم.
- سپس وارد پوشه ی **BranchCache** شده و ابتدا وارد گزینه ی **Turn On BranchCache** شده و **Enable** می کنیم. به این شکل به همه ی **Client** ها و **Server** های موجود در شبکه، اعلام می شود که قابلیت **BranchCache** را فعال کنند.
- سپس چون نوع **Hosted Cache Mode** را **Implementation** می کنیم، گزینه ی **..Set BranchCache Hosted** را باز و **Enable** کرده و در کادر پایین، **IP** یا نام **Hosted Cache Server** را (**DC3**) بصورت **FQDN** درج می کنیم. در غیراینصورت، باید گزینه ی **..Set BranchCache Distributed** را **Enable** می کردیم.
- حال وارد گزینه ی **..Enable Automatic Hosted Cache Discoverd by Service** را شده و **Enable** می کنیم. به این شکل، **Client** ها می توانند به طور خودکار سیستم **Host** را شناسایی کنند.
- سپس وارد گزینه ی **Configure BranchCache for Network files** شده و آن را **Enable** کرده و در کادر پایین مقداری را بر حسب میلی ثانیه تعیین می کنیم که برای **Client** ها تعیین می کند که اگر تأخیر در دریافت هرنوع فایلی، بیش از این میزان بود، آن را **Cache** کند که اگر این مقدار صفر باشد، در نتیجه همه ی فایل های دریافتی را **Cache** می کند.
- از طریق گزینه ی **..Set Percentage of disk space** می توانیم میزان استفاده ی هر **Client** از حافظه، جهت **Cache** گیری را تعیین کنیم و تمام!
- برای تأثیرگذاری سریعتر این **Policy** ها، در همه ی **Server** ها و **Client** ها، دستور **gpupdate /force** را وارد می کنیم.
- پس از اینکه در **Client** ها هم **gpupdate** را زدیم، با دستور **Get-BCStatus** می بینیم که قابلیت **BrachCach** نیز فعال است.

5. قابلیت BranchCache را تست می کنیم.

- در حقیقت، در عمل، فایلهایی که بصورت معمولی **Share** شده اند، با فایل هایی که دارای قابلیت **BranchCache** هستند، تفاوت خاصی ندارند.
- تفاوت، تنها در سرعت استفاده ی آنهاست.
- مثلاً اگر در سیستم **PC1**، فایل **Share** شده ی **DC1** را برداشته و برای خودمان کپی کنیم و یکبار حذف کنیم، بار بعد که بخواهیم آنرا دوباره کپی کنیم، با سرعت خیلی بالاتری دریافت می شود، چون آن فایل هنوز در **Cache** سیستم **DC3** موجود است.

- برای اینکه استفاده از **Cache Server** را ببینیم، در همان **PC1** می توانیم کنسول **Performance Monitor** را باز کرده و در کادر سمت چپ وارد پوشه ی **Monitoring Tools** و سپس **Performance Monitor** شده و بر روی علامت + کلیک می کنیم؛ سپس در کادر سمت چپ، گزینه ی **BranchCache** را انتخاب و **Add** کرده و **OK** می کنیم. حال از ابزارهای بالای برنامه، بر روی **Change Graph Type** زده و گزینه ی **Report** را انتخاب می کنیم. حال می توانیم یک فایل را برای اولین بار از **Content Server** (**DC1**) درون این **Client** کپی کرده و به تغییرات مقادیر در این آمار دقت کنید. همچنین به ثابت ماندن این مقادیر در دفعات بعدی که آن فایل ها را دوباره کپی می کنید، دقت کنید!

NIC Teaming :

به این قابلیت، **NIC Bonding** و **Network Adapter Teaming** نیز گفته می شود.
قابلیتی است که در طی آن، یک **Server** فیزیکی یا مجازی دارای چندین کارت شبکه، با آدرس های متفاوت است که با یکدیگر متحد یا ترکیب شده اند و تشکیل یک کارت شبکه ی واحد را می دهند که برای **Client** ها، تنها یک آدرس به نظر می رسد.
به دلایل زیر انجام می گیرد:

- افزایش کارایی یا **Throughput**
- افزایش پهنای باند یا **Bandwidth**

مثلاً اگر دو کارت شبکه با سرعت **1 GBps** داشت باشیم، وقتی **Team** می شوند، یک کارت شبکه با سرعت **2Gbps** نخواهیم داشت! بلکه دو مسیر **1Gbps** خواهیم داشت که موجب ایجاد **Load Balancing** برای ترافیک می شود.

- افزایش میزان **Failover**

اگر یکی از **NIC** ها از کار بیفتد، سایر **NIC** ها به کار خود ادامه داده و مانع **down** شدن ارتباط **Server** می شوند.

- ❖ اهمیتی ندارد که کارت شبکه ها از یک سازنده و یک مدل باشند یا نباشند.
- ❖ حتی گاهی توصیه می شود که **NIC** های عضو تیم، از سازندگان مختلف باشند تا چنانچه یکی یا بعضی از آنها دارای مشکل **Driver** باشند (در رابطه با سازگاری با ویندوز)، بقیه کار را انجام دهند.
- ❖ نکته ی مهم این است که **Driver** کلیه کارت های شبکه ی عضو تیم، حتما به درستی نصب شوند و نه از روش هایی مانند **plug and play** و یا برنامه هایی مثل **Driver Pack Solution**!
- ❖ می توان تا **32** عدد **NIC** را تیم کرد.
- ❖ توصیه می شود که بهتر است **Server** حداقل دارای **NIC** باشد که با یکدیگر تیم باشند و ترجیحا به دو سوئیچ مختلف وصل باشند که حتی اگر یکی از سوئیچ ها هم دچار مشکل شد، کارت دیگر که به سوئیچ دیگر متصل است، کار را ادامه دهد.

اولین پیشنیاز برای راه اندازی **NIC Teaming** این است که **Switch** های متصل به **Server** هم قابلیت **NIC Teaming** را پشتیبانی کنند. که به صورت **SW Teaming** نشان داده می شود.

NIC Teaming شامل دو پیکربندی می شود:

- ❖ **Teaming Mode:**

که شامل سه نوع است:

1. **Static Teaming** :

- ➢ در این حالت باید تمام اعضای **Team** به یک **Switch** فیزیکی وصل شده و **Config** هایی نیز روی این **Switch** اعمال شود.
- ➢ پس باید درگاه **Ethernet** خود **Switch** فیزیکی و نیز خود **Server** را بصورت دستی پیکربندی کنیم.
- ➢ البته چنانچه تعدادی **Management Switch** داشته باشیم که به یکدیگر متصل باشند، می توان **NIC** ها را به این **Switch** های مختلف نیز وصل کرد.
- ➢ این الگوریتم یک مدل عمومی برای **Load Balance** است که افزایش پهنای باند و **Fault Tolerance** را ساده‌تر انجام می دهد.
- ➢ این حالت به **Generic Teaming** نیز معروف است.
- ➢ سوئیچ باید از نوع **Server-class** باشد، یعنی باید حتماً این قابلیت را پشتیبانی کند.

2. **Dynamic Teaming** یا LACP (Link Aggregation Control Protocol):

- بسیار کارآمدتر از **Static Teaming** است.
- در این مدل **Switch** متصل به **NIC** حتما باید **Config** شود و **Port** های **Switch**، در داخل یک **EtherChannel** قرار داده شوند. **EtherChannel**که از نوع **LACP** باشد.
- در این روش **Server** و **Switch** با هماهنگی میان یکدیگر، مشخص می کنند که آیا یک **Port** در داخل **Team** قرار می گیرد یا خیر.
- اگر برای **Port** یکی از طرفین، مشکلی ایجاد شود، **Port** همسان در طرف مقابل، متوجه شده و به صورت خودکار، از تیم خارج می شود تا از بروز مشکل در ارتباط، جلوگیری کند.
- **Switch** باید حتماً این قابلیت را پشتیبانی کند.

3. **Switch Independent** :

- ساده ترین حالت است که برای اجرای **NIC Teaming** برای **Virtual Machine** ها، تنها از این حالت استفاده می شود.
- در این حالت، **NIC** ها مستقل از **Switch** کار می کنند و نیازی به **Config** آنها نیست.

❖ **Load Balancing Mode :**

که شامل سه نوع است:

1. **Address hashing** :

- اگر در شبکه ی خود، از پروتکل **IPsec** استفاده نمی کنیم، بهتر است برای **Load Balancing** این گزینه را انتخاب کنیم.
- در این روش، ترافیک خروجی از تمام **NIC** های فعال، ارسال می‌شود، اما ترافیک ورودی فقط از یک **NIC** دریافت می‌شود.
- در واقع **Load Balancing** فقط روی ترافیک خروجی اعمال می شود.
- این حالت توسط رمزگذاری یا **hash** کردن مشخصات **Packet** ارسالی، مثل**IP** ، **MAC** ، **Port Number** تعیین می کنند که بسته از کدام **Interface** ارسال شود.
- به این صورت که **Packet** های ارسالی با یک مقدار **hash** مخصوص، به یکی از **NIC** های عضو **Team**، فرستاده می شوند.
- حالت **Address Hashing**، مناسب برای **Server** هایی است که اغلب ترافیک آنها بصورت خروجی است، مثل **Web Server** ها.
- این نوع از **Load balancing**، تنها حالت مجاز برای اجرای **NIC Teaming** برای ماشین های مجازی در **HyperV** می باشد، که شامل سه حالت است:
  - **TransportPorts**
  - **IPAddresses**
  - **MacAddresses**

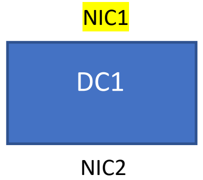
2. **Hyper-V** :

- مناسب برای محیط های مجازی که شامل **Virtual Machine** ها و **Virtual Switch** ها هستند، می باشد.
- این ارتباط به ماشین مجازی وابسته نیست، بلکه به **Virtual NIC** وابسته است.
- از این حالت زمانی استفاده می شود که در شبکه، یک **Host** برای مجازی سازی توسط **Hyper-V** در شبکه وجود داشته باشد که میزبان یک یا چند **Virtual Machine** می باشد.

3. **Dynamic** : به صورت ترکیبی از دو حالت قبل عمل می کند.

Address Hashing NIC Teaming :

فرض کنید DC1، دارای دو کارت شبکه ی متصل و روشن، به صورت روبرو می باشد.
NIC1 به مودم اینترنت متصل است و NIC2 به شبکه ی داخلی متصل شده است.
حال می خواهیم ارتباط این DC با شبکه را توسط این دو کارت شبکه انجام دهیم.



- کنسول Server Manager را باز کرده و در تب Local Server بر روی لینک روبروی NIC Teaming که بصورت Disable نشان داده می شود، کلیک می کنیم.
- در کادر سمت راست، پایین، NIC ها را می بینیم، اگر تعداد آنها بیشتر هم می بود، می توانستیم بطور دلخواه دو یا چند عدد از آنها را انتخاب کرده و از منوی بالای آن TASKS، گزینه ی Add to new Team را می زنیم.در اینجا هردو را انتخاب می کنیم.
- یا اینکه در کادر سمت چپ، پایین، بر روی TASKS زده و وارد New Team شده و NIC های موردنظر را اضافه می کنیم.
- یک نام درج کرده و روی Additional properties در پایین، کلیک کرده و چون Switch واقعی نداریم و در محیط آزمایشی هستیم، برای Teaming mode گزینه ی Switch Independent را می زنیم.
- برای Load Balancing گزینه ی Address Hash را انتخاب می کنیم.
- اگر چند NIC داشته باشیم، و فعلاً بخواهیم یکی از NIC های عضو Team را استفاده نکنیم، اما به عنوان آماده باش قرار بگیرد، می توان برای گزینه ی Standby adapter آن را انتخاب کرد و OK!
- حال اگر وارد پنجره ی Network Connections شویم، می بینیم که یک آداپتور Teaming اضافه شده است.
- اگر وارد تنظیمات Adapter های دیگر شویم، می بینیم که گزینه ی IPv4 همه ی آنها غیرفعال شده است!
- پس باید IP Address ای که برای آداپتور Server تعیین کرده بودیم را برای NIC تیم شده، تنظیم کنیم؛ پس وارد تنظیمات IPv4 آن شده و انجام می دهیم.
- حال برای تست این ارتباط، وارد PowerShell شده و مثلاً دستور زیر را وارد می کنیم:

```
Test-NetConnection www.google.com
```

Failover Clustering :

Failover Cluster، یعنی گروهی متشکل از حداقل دو کامپیوتر (فیزیکی / مجازی) که یک **Application** به طور مشترک روی آنها اجرا می شود.

تمام این گروه، به عنوان یک نهادِ واحد، شناخته شده و عمل می کند.

بزرگترین مزیت **Failover Cluster** این است که **High Availability** را در شبکه به بالاترین سطح می رساند.

منظور از **High Availability** قابلیتهای زیر می باشد:

- **Fault Tolerance** (تحمل خطا)
- **Network Load Balancing** (تقسیم بار شبکه)

مثلاً فرض کنید که در یک شبکه قرار است که **Web Hosting** داشته باشیم.

حال فرض کنید فقط یک **Web Server** داشته باشیم.

اگر این **Server** دچار مشکل (سخت افزاری / نرم افزاری) شود؛ فرآیند **Web Hosting** در شبکه متوقف خواهد شد.

توسط **Failover Clustering**، می توانیم چند **Web Server** داشته باشیم و آنها را درون یک **Failover Cluster** قرار دهیم که پشتیبان یکدیگر باشند و سطح **High Availability** را بالا نگه دارند.

در حالت **Failover Clustering**، در ظاهر، شبکه دارای فقط یک **Web Server** با یک آدرس **IP** مشخص است، اما در واقع چندین **Web Server** در حال اجرای نرم افزار و سرویس دهی می باشند.

- هر کدام از کامپیوترهای عضو **Failover Cluster** را **Node** می گوییم.
- **Failover Cluster** قابلیت توسعه دارد یعنی می توان همواره **Node** های آنرا کم یا زیاد کرد.
- هر **Failover Cluster** می تواند **حداکثر شامل 64 کامپیوتر** فیزیکی باشد.
- این کامپیوترهای فیزیکی می توانند **Hyper-V Server** هم باشند و حداکثر **1024** ماشین مجازی داشته باشند.
- اما به طور کل، یک **Failover Cluster** می تواند **حداکثر شامل 8000 ماشین مجازی** باشد.
- بهتر است که مقدار **RAM** و **CPU** همه ی **Node** ها یکسان باشند.
- پیکربندی **NIC** های **Node** ها باید یکسان باشد.
- **Version** و **Edition** سیستم عامل همه ی **Node** ها باید یکسان باشد.
- همه ی سیستم عامل ها باید **Update** های یکسان دریافت کنند، به همین دلیل همه ی **Node** ها را درون یک **WSUS Computer Group** قرار می دهیم.
- برنامه ای که قرار است همه ی **Node** ها آن را اجرا کنند، باید در همه ی آنها، نسخه و نگارش یکسان داشته باشد.
- **Failover Cluster** را هم به صورت گرافیکی توسط کنسول **Failover Cluster manager** و هم توسط **PowerShell** می توان مدیریت کرد.
- بهتر است که یک **Storage** مشترک مثل **NAS** یا **SAN** را به **Failover Cluster** اختصاص دهیم که همه ی **Node** ها بطور همزمان و یکسان، به فایل های یکسان دسترسی داشته باشند.
- نمی توان **DAS** را به **Failover Cluster** اختصاص داد.

- بهترین **Storage** های قابل استفاده به ترتیب:
  - ✓ **FcSAN**
  - ✓ **SAS**
  - ✓ **ISCSI**
  - ✓ **Shared VHD Set** (در **HyperV**)

ایجاد Isolation و حذف Point of Failure :

- در حقیقت Failover Cluster بطورکلی به شبکه ی اصلی سازمان متصل خواهد بود، اما برای ارتباط میان Node ها بهتر است که یک شبکه ی مختص آنها داشته باشیم.
- پس در راه اندازی استاندارد Failover Cluster، هر کدام از Node ها حداقل دارای سه NIC می باشند:
  - یکی برای اتصال به شبکه ی Failover Cluster
  - یکی برای اتصال به SAN یا NAS
  - یکی برای اتصال به شبکه ی LAN سازمان
- از آنجایی که استفاده از فقط یک Switch در شبکه، خودش یک Point of Failure است.
- بجای استفاده از یک Switch (هرچند قدرتمند) و VLAN بندیِ آن و اختصاص یک VLAN به هریک از شبکه ها، از Switch های فیزیکی به ازای هر شبکه استفاده می کنیم.
- استفاده از NIC Teaming

انواع طرح های پیاده سازی Failover Cluster :

- Single Domain Cluster : در این Plan ، همه ی Node های Failover Cluster عضو یک Domain هستند.
- Multi-Domain Cluster : Node های Failover Cluster، عضو Domain های مختلفی هستند.
- Workgroup Cluster : Node های یک Failover Cluster عضو هیچ Domain ای نیستند.

توصیه می شود که Failover Cluster بصورت Single Domain Cluster پیاده سازی شود.

- ✓ البته راه اندازی یک Cluster برای ارایه ی برنامه هایی مثل SQL Server در محیط غیر AD DS و در نتیجه در طرح Workgroup Cluster بدون کوچکترین مشکل، می توانند کار کنند، چون دارای مکانیزم احراز هویت اختصاصی خود می باشد.
- ✓ اما یک File Server Cluster بدون AD DS به مشکل بر می خورد!

Quorum :

ابزاری است که میزان قابل قبول Failure یا Node های از دست رفته را تعیین و کنترل می کند.

به این صورت که به هر Node یک Vote یا شماره می دهد، و از طرف دیگر این قانون را کنترل می کند که تا زمانی که تعداد Vote های موجود، از تعداد 50 درصد Node های شبکه به اضافه ی یک، بیشتر باشد، مشکلی ندارد، اما اگر کمتر باشد، یعنی این Cluster نمی تواند به خوبی کار کند، پس باید Stop و Down شود.

فرض کنید که یک Cluster شامل چهار Node می باشد، و دو Node از کار می افتند، پس تعداد Vote ها از میزان قابل قبول (2 + 1) کمتر شده است، پس Cluster از کار می افتد.

ما می توانیم از یک عنصر به نام Witness استفاده کنیم و به آن هم یک Vote اختصاص دهیم تا در مواقع اینچنینی باعث برپا نگه داشتن Cluster شود.

Witness می تواند یکی از سه حالت زیر باشد:

- **Disk Witness :**
  - برای Cluster هایی مناسب است که دارای Shared Storage هستند اما Replication میان آنها برقرار نیست و اگر برقرار باشد، نمی توان از Disk Witness استفاده کرد.
  - باید یک دیسک خام و خالی و با حداقل اندازه ی 512MB و با فرمتبندیِ Basic باشد و فقط یک Partition داشته باشد.
  - باید آن را مخصوص Cluster تعیین کنیم و نه Role مربوط به Cluster (مخصوص Witness)
  - باید به عنوان Clustered Storage استفاده شود.
  - می تواند NTFS یا ReFS باشد و می تواند عضو یک hardware Raid هم باشد.
  - درون نرم افزارهای Antivirus و Backup موجود در سیستم، باید excluded شده باشد.

- **File Share witness (SMB Share):**
  - **یک فایل log است که شامل اطلاعات Cluster می باشد، اما به بانک داده های Cluster دسترسی ندارد.**
  - **برای Multi-Domain Cluster ها مناسب است.**
  - **باید حداقل 5MB فضای خالی داشته باشد.**
  - **باید دارای Write Permission باشد.**

- **Cloud Witness :**
  - **مناسب برای Cluster های میان Data Center های مختلف در Remote Site هاست که یک Witness مستقل از Data Center ها محسوب می شود.**
  - **تحت Microsoft Azure استفاده می شود.**

تنظیمات امکانپذیر برای Clustering :

- **Node Majority :**
  - **برای Cluster های با تعداد Node های فرد مناسب است.**
  - **Witness وجود ندارد.**
  - **میزان Failure را تا میزان تعداد نیمی از Node ها منهای یک، می تواند بپذیرد.**
  - **مثلاً در صورت داشتن هفت Node، می تواند تا سه Failed Node را بپذیرد و Cluster را از کار نیندازد.**

- **Node and Disk Majority :**
  - **برای Cluster های با تعداد Node های زوج مناسب است.**
  - **میزان Failure را تا میزان تعداد نیمی از Node ها، می تواند بپذیرد، که پیشنیاز آن، Online بودن Disk Witness است، چراکه خود Disk Witness دارای یک Vote خواهد بود.**
  - **مثلاً در صورت داشتن شش Node، می تواند تا سه Failed Node را بپذیرد و Cluster را از کار نیندازد.**
  - **اما در صورت Fail شدن Disk Witness، فقط می تواند تا دو Failed Node را بپذیرد.**

- **Node and File Share Majority :**
  - **مشابه با حالت Node and Disk Majority عمل می کند، اما از File Share Witness استفاده می کند.**
  - **باید حداقل یکی از Node ها شامل یک کپی از اطلاعات تنظیمات Cluster باشد؛ در غیراینصورت باید به صورت manual تعیین کنیم که Cluster توسط کدام Node روشن شود.**

- **No Majority : Disk Only :**
  - **بدترین و بی استفاده ترین نوع است.**
  - **تا زمانی که حداقل یک Node روشن و سالم باشد، همه ی Failure ها را می پذیرد و Cluster را down نمی کند.**

نکته: اگر Node های Cluster در مکان های متفاوتی واقع شده باشند، باید تا جایی که امکانپذیر است، سعی کنیم Node حاوی Wittnes را در مکانی متفاوت از مکان Node های عضو Cluster قرار دهیم.

: Dynamic Quorum

در این حالت، اگر تعداد Failed Node ها از تعداد مجاز بیشتر شود، Quorum آن Node ها را بطورکامل از تنظیمات Cluster حذف می کند، طوری که گویی از ابتدا آنها وجود نداشتند، و به این شکل، کار را با Node های موجود ادامه می دهد که Cluster قطع نشود. و این کار را تا زمانی که فقط یک Node باقی بماند، ادامه می دهد.

: Dynamic Witness

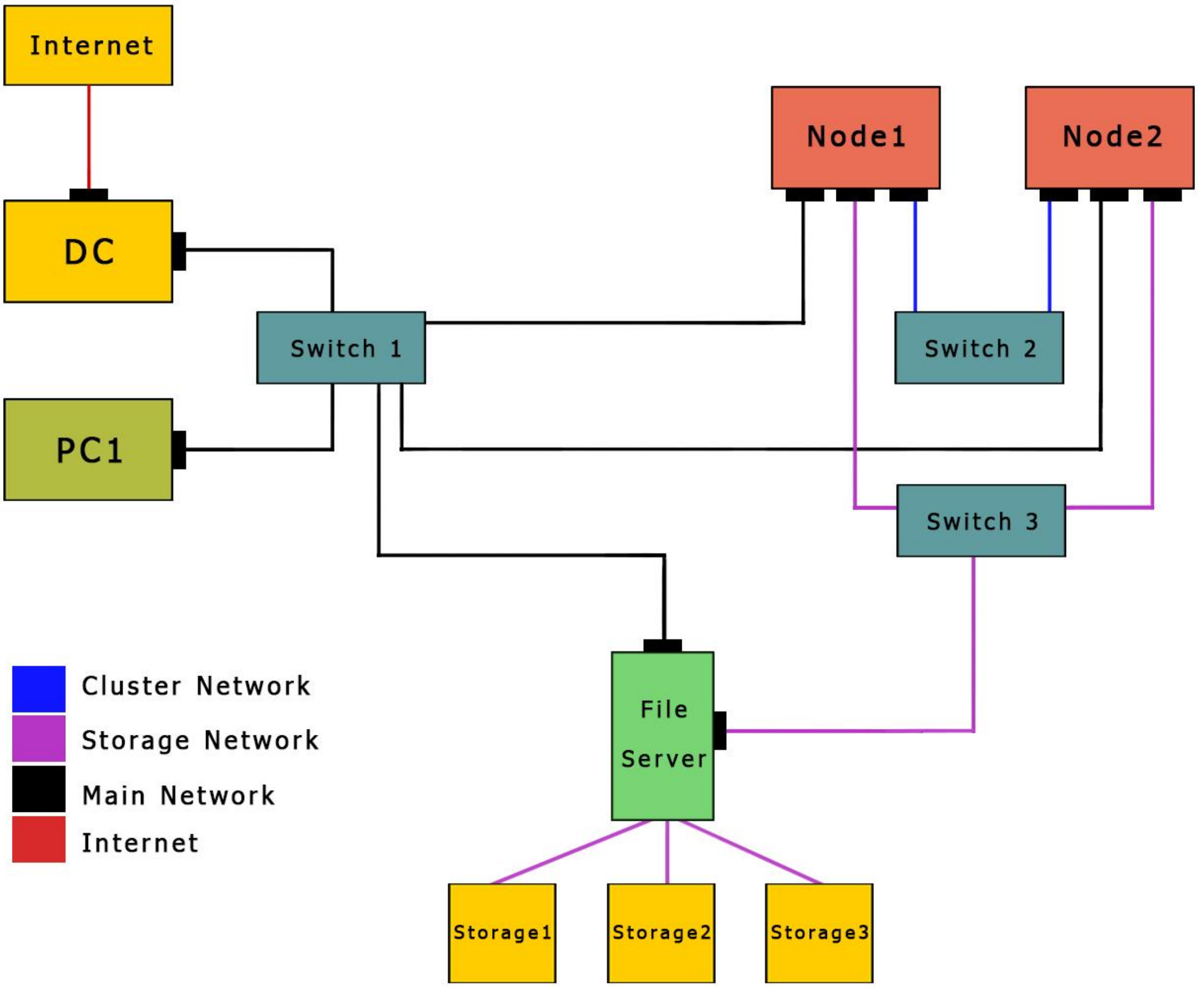
در این شیوه، دو حالت وجود دارد:

- **زمانی که تعداد Node ها زوج باشد: Witness یک Vote به خودش اختصاص می دهد.**
- **زمانی که تعداد Node ها فرد باشد: Witness هیچ Vote ای به خودش اختصاص نمی دهد.**

و این اختصاص و حذف Vote به Witness، تا زمانی که فقط یک Node باقی بماند، ادامه می یابد.

نکته: با راه اندازی یک Cluster در ویندوز Server، بطورخودکار هم dynamic Quorum و هم dynamic Witness فعال می شوند.

Implement a Failover Clustering :



- در نمودار بالا:
  - Node های یک و دو، دو سیستم با Windows Server هستند که عضو Domain و AD شده اند و هریک دارای سه NIC است.
  - File Server نیز یک سیستم با Windows Server است.
- شبکه ی اصلی، بطور فیزیکی، به تک تک همه ی اعضای یک Cluster متصل می شود، اما از لحاظ منطقی، همه ی آنها را یکی خواهد دید.
- پس برای راه اندازی یک Cluster در شبکه، بطور ظاهری، همه ی اعضای Cluster مثل Member Server های معمولی، به شبکه متصل می شوند. اما در پشت زمینه ی شبکه، بین آن Server های موردنظر، یک شبکه ی خصوصی راه اندازی می کنیم و آنها را عضو یک Cluster می کنیم.
- ارتباط اعضای شبکه ی Cluster با File Server باید شامل ویژگی های زیر باشد:
  - ❖ مجزا از شبکه ی Clustering خودشان
  - ❖ مجزا از شبکه ی اصلی

1. File Server را آماده می کنیم.

نکته: قبل از آغاز این فرآیند، ضروری است که همه ی اعضای شبکه را کاملاً به روز رسانی کرده باشیم.

نقش مربوط به File Server را روی سیستم درنظرگرفته شده به عنوان File Server، نصب می کنیم.

(در تب Select Server roles، گزینه ی iSCSI Target Server را انتخاب می کنیم و تا پایان پیش می رویم.)

در DC به Server manager به بخش File and storage services رفته و در پنجره ی آن روی آیتم سیستم File Server کلیک راست کرده و iSCSI Target Settings را می زنیم.

در پنجره ی باز شده، تنها گزینه ای که آدرس شبکه ی میان Node ها و File Server را نشان می دهد را فعال می کنیم و OK.

2. قابلیت iSCSI Initiator را بر روی هریک از Node ها راه اندازی می کنیم.

- در خورد سیستم DC وارد PowerShell شده و به ترتیب دستورات زیر را وارد می کنیم:

```
Invoke-Command Node1,Node2 {Get-Service *iscsi* | Set-Service -StartupType Automatic
-PassThru | Start-Service}
```

- برای اطمینان از اینکه صحیح اجرا شده است، و یک آدرس به iscsi target اختصاص داده شده است، دستور زیر را وارد می کنیم:

```
Invoke-Command Node1,Node2 {Get-InitiatorPort}
```

در پاسخ، باید در نمایش مشخصات Node ها، برای هریک از آنها، گزینه ای به نام NodeAddress وجود داشته باشد که شامل یک آدرس iqn می باشد.

- در هریک از Node ها، یک iSCSI target portal تعریف می کنیم:

```
Invoke-Command Node1,Node2 {New-IscsiTargetPortal -TargetPortalAddress x.x.x.x}
```

پس برای آدرس IP، آدرس سیستم File server را می دهیم.

3. دو iSCSI lun یا حافظه ی مجازی را در درایو موردنظر موجود در File Server ایجاد می کنیم، یکی برای ذخیره سازی و یکی بعنوان witness!

```
Invoke-Command File-Server {New-IscsiVirtualDisk -Path D:\Node-DataDisk.vhdx -SizeBytes 100GB}
Invoke-Command File-Server {New-IscsiVirtualDisk -Path D:\Node-QuorumDisk.vhdx -SizeBytes 1GB}
```

همانطور که در نتیجه به چشم می خورد، Lun های ایجاد شده، از نوع dynamic خواهند بود؛ یعنی حجم اولیه ی دیسک، برابر با 100 یا یک گیگابایت نخواهد بود، و با افزایش حجم محتویات آنها، حجم Virtual Disk هم زیاد خواهد شد.

4. یک iSCSI Server Target در سیستم file server ایجاد می کنیم.

```
Invoke-Command File-Server {New-IscsiServerTarget -TargetName Node-Target
-InitiatorIds "IPAddress:x.x.x.x","IPAddress:x.x.x.x"}
```

یک نام برای Server Target درج کردیم و برای آدرس های IP، آدرس IP های Node ها در شبکه شان با File Server را می دهیم.

5. iSCSI lun ها را به iSCSI Server Target اختصاص می دهیم.

```
Invoke-Command File-Server {Add-IscsiVirtualDiskTargetMapping -TargetName Node-Target
-Path D:\Node-DataDisk.vhdx}

Invoke-Command File-Server {Add-IscsiVirtualDiskTargetMapping -TargetName Node-Target
-Path D:\Node-QuorumDisk.vhdx}
```

6. حال iSCSI target portal را به روزرسانی می کنیم.

```
Invoke-Command Node1,Node2 {Get-IscsiTargetPortal | Update-IscsiTargetPortal}
```

حال اگر بر روی هریک از Node ها دستور درخواست مشاهده ی iSCSI Target را وارد کنید، مشخصات آن را دریافت خواهید کرد، که البته از درون DC تنها با دستور زیر می توان آنها را مشاهده کرد:

```
Invoke-Command Node1,Node2 {Get-IscsiTarget}
```

7. initiator های هردو Node را به Target متصل می کنیم.

```
Invoke-Command Node1,Node2 {Get-IscsiTarget | Connect-IscsiTarget}
```

برای اینکه این اتصال پایدار باقی بماند و با یک restart از بین نروند:

```
Invoke-Command Node1,Node2 {Get-IscsiSession | Register-IscsiSession}
```

حال اگر به Server manager و Volumes و سپس به Disks برویم و یکبار refresh کنیم، می بینیم که هر دو Node اضافه شده اند و برای هریک، هردو Lun یا دیسک مجازی که ایجاد کردیم، متصل شده اند که البته همچنان offline هستند که باید آنها را روشن کنیم.

پس هرتغییری که بر روی یکی از Lun ها در یکی از Node ها ایجاد کنیم، بر روی آن Lun در Node دیگر نیز ایجاد خواهد شد.

روی هریک از Lun ها:

- کلیک راست کرده و bring online را می زنیم.
- دوباره کلیک راست کرده و initialze را می زنیم.
- دوباره کلیک راست کرده و New Volume را می زنیم، و ویزارد را طی می کنیم و تمام!

حال اگر یکبار refresh کنیم، می بینیم که برای Node دیگر نیز تغییر کرده اند.

8. Feature مربوط به Failover clustering را بر روی Node ها راه اندازی می کنیم.

```
Invoke-Command Node1,Node2 {Install-WindowsFeature Failover-Clustering}
```

Cluster را بر روی Node ها تست می کنیم که باید نتیجه ی مثبتی داشته باشد؛ هم از نظر شبکه و هم از نظر storage:

```
Test-Cluster -Node Node1,Node2
```

9. Cluster را ایجاد می کنیم.

باید دقت کنیم که لازم خواهد بود یک IP به این Cluster اختصاص دهیم (که مجازی خواهد بود)، که جهت ارتباط با Cluster بکار گرفته خواهد شد و در شبکه ای که میان File server و DC و همه ی Node هاست، باشد.

حتماً در Server manager چک می کنیم که همه ی دیسک های روی Node ها به صورت online هستند.

از طریق GUI:

- وارد Server manager شده و از منوی Tools گزینه ی Failover Cluster Manager را می زنیم.
- در کنسول باز شده، در سمت چپ، بر روی آبجکت Failover Cluster Manager کلیک راست کرده و Validate Configuration را می زنیم.
- در تب Select Servers or a Cluster، یکی یکی نام کامل Node ها را وارد و Add می کنیم: Node1.payamavar.local و ...
- گزینه ی Run all tests را انتخاب کرده و Test را start می کنیم.
- در نتیجه، باید مقابل هردو Node عبارت validated درج شده باشد، و وقتی روی view Reports کلیک می کنیم، در صفحه ی باز شده، مقدار Result Summary برای همه ی گزینه ها، با رنگ سبز نشان داده شده باشند. اگر برای یکی یا برخی از گزینه ها، نشانه ی اخطار زرد رنگ درج شده بود، باید وارد Node ها شده و سیستم عامل آنها را update کرد و دوباره به این wizard برگشت و از نو تست کرد.
- وقتی همه نتایج در view report سبز رنگ بود، در پایان ویزارد باز شده، گزینه ی Create the cluster now using the validated nodes را فعال کرده و finish را می زنیم، که یک Wizard دیگر باز می شود. یک نام برای این cluster درج می کنیم، مثلاً: myCluster و یک IP برای آن درج می کنیم و ویزارد را به پایان می بریم.
- برای تست اینکه Cluster فعال شده است، در همین کنسول، و در کادر میانی کنسول، گزینه ی Validate Cluster را می زنیم.

از طریق PowerShell:

- اگر شبکه مان شامل یک domain باشد:

```
New-Cluster -Name myCluster -Node Node1,Node2 -StaticAddress x.x.x.x
```

✓ در این حالت یک Onject در AD برای این Cluster ایجاد خواهد شد.

- اگر شبکه مان شامل بیش از یک domain باشد:

```
New-Cluster -Name myCluster -Node Node1,Node2 -StaticAddress x.x.x.x
-AdministrativeAccessPoint Dns
```

- ✓ اگر در AD به OU مربوط به **Computers** برویم، می بینیم که یک **Object** برای **Cluster** موردنظر ایجاد شده است.
- ✓ اگر وارد کنسول **DNS** شویم، می بینیم که که **A Record** برای این **Cluster** ایجاد شده است.

نکته: اگر این A Record ایجاد نشده باشد، به کنسول Failover Cluster Manager برگشته و در پایین کادر میانی، بر روی آبجکت Cluster در نوار Server Name، کلیک راست کرده و Take offline را زده و پس از چند ثانیه دوباره کلیک راست کرده و اینبار more Actions و سپس Repair را می زنیم.

- ✓ اگر وارد **Server manager** و تب **All Servers** شویم، می بینیم که آبجکت **Cluster** نیز اضافه شده است.
- ✓ وارد کنسول **Failover Cluster Manager** شده و در سمت چپ، بر آبجکت **Failover Cluster Manager** باز می کنیم.

- ○ وارد **Storage** و سپس **Disk** می شویم، تا **Lun** ها را ببینیم؛ می توانیم نام آنها را بطورمشخص تر تعیین کنیم، پس با راست کلیک روی هریک و انتخاب **Properties** …

- ○ وارد **Networks** می شویم تا شبکه های موجود را مشاهده کنیم و در صورت نیاز اسامی آنها را تغییر دهیم. ، مثلاً برای شبکه ای که میان **Node** هاست: یک نام مشخص و برای شبکه ای که میان همه ی اعضای شبکه ست، یک نام مشخص دیگر و …

نکته: اگر از قبل دیسک ها را پیکربندی نکرده و یا Quorum را مشخص نکرده بودیم، می توانستیم در همین کنسول، بر روی آبجکت Cluster در کادر سمت چپ، راست کلیک کرده و more actions را زده و سپس Configure Cluster Quorum settings را بزنیم.

- ✓ مثلاً اگر بخواهیم همین **witness** ای که در بالا ایجاد کردیم در ویزارد باز شده ایجاد کنیم، گزینه ی **Select the quorum witness** را زده و سپس **Configure a disk witness** را می زنیم.
- ✓ برای انتخاب **Cloud witness** نیاز است که یک حساب **Microsoft Azure** داشته باشیم.
- ✓ همانطور که می دانیم، در یک **Cluster**، همه ی **Disk** ها یک **Vote** خواهند داشت، اگر قصد داشته باشیم، که یکی یا برخی از آنها هیچ **Vote** ای نداشته باشند، گزینه ی **Do not configure a quorum witness** را انتخاب کرده و پیش می رویم.

: Cluster update

برای اینکه Cluster را طوری تنظیم کنیم که به طور خودکار update یا به روزرسانی شود (self update):

- ▪ **وارد کنسول Failover Cluster Manager شده و در کادر سمت چپ، روی آبجکت Cluster کلیک راست کرده و more actions و سپس Cluster-Aware Updating را می زنیم.**
- ▪ **در پنجره ی باز شده، در سمت راست، Analyze cluster updating readiness را می زنیم.**
  - ➢ **اگر گزینه ی firewall سبز نشده بود، باید Rule مربوط به آن را در Firewall شبکه فعال کنیم.**
  - ➢ **اگر گزینه ی مربوط به Proxy server را به صورت waning نشان داد، درصورتی که هیچ proxy server ای در Cluster تعریف نشده باشد، اهمیت زیادی هم نخواهد داشت.**
  - ➢ **اگر گزینه ی مربوط به CAU (Cluster automatically update) هم به شکل warning باشد، به این دلیل است که ابتدا باید این قابلیت را بر روی تک تک Node ها راه اندازی کنیم:**

```
Invoke-Command Node1,Node2 {Install-WindowsFeature rsat-clustering -IncludeAllSubFeature}
```

- ▪ **حال در همان پنجره ی Cluster-Aware updating وارد گزینه ی Configure cluster self-updating options می شویم و در ویزارد ظاهر شده، گزینه ی Add the CAU clustered role را نیز فعال می کنیم و در تب بعد، می توانیم زمانبندی را بطور دلخواه جهت self updating تنظیم کنیم؛ و بقیه ی تب ها را فعلاً بدون تغییر رها کرده و تا پایان می رویم.**
- ▪ **جهت غیرفعال و یا حذف کردن این self updating، می توان دوباره روی گزینه ی Configure cluster self-updating options کلیک کرد.**
- ▪ **درحقیقت update غیر خودکار و دستی به این صورت است که در همان پنجره ی Cluster-Aware Updating روی گزینه ی Apply updates to this cluster کلیک کنیم و ویزارد را بطورمشابه پیش ببریم.**

نکته: گاهی پس از اینکه سیستم را یکبار خاموش روشن می کنیم، در کنسول **Failover Clustering**، و در آبجکت **Cluster Events**، یک سری خطا مشاهده می کنیم! برای رفع آنها، می توان در کادر سمت راست، یکبار گزینه ی **Reset Recent Events** را زد.

Node change:

فرض کنید یکی از **Node** ها دارای یک سیستم عامل قدیمی تر از سیستم عامل های دیگر موجود در شبکه است، مثل **win.Server.2012**. برای اینکه سیستم عامل آن را **upgrade** کنیم:

- ابتدا در کنسول **Failover Cluster Manager** در سمت چپ، وارد **Nodes** می شویم.
  - سپس آن را **stop** می کنیم: در کادر میانی بر روی **Node** موردنظر کلیک راست کرده و **Pause** و سپس **Drain Roles** را می زنیم.
  - آن را اخراج می کنیم: دوباره روی آن کلیک راست کرده و از **more Actions** گزینه ی **Evict** را می زنیم.
- حال بر روی همان **Node**، ویندوز را ارتقا می دهیم، مثلاً **Windows erver 2019** را نصب می کنیم.
- تمامی **Role** ها و **feature** های موردنیاز **Clustering** را از نو روی آن نصب می کنیم.
- در سیستم **DC** وارد **Failover Slustering Manger** شده و در سمت چپ آبجکت **Cluster** را انتخاب کرده و در کادر میانی، گزینه ی **Add Node** را می زنیم؛ در نوار **Enter Server name** نام **Node** به روز شده را وارد و **Add** می کنیم و ویزارد را به پایان می بریم.
- حال اگر به آبجکت **Node** برگردیم، می بینیم که **Node** جدید، اضافه شده است.
- حال نیاز است که **Functional Level** مربوط به **Cluster** را نیز ارتقا دهیم، پس به **Power Shell** می رویم.

می توا ابتدا توسط دستور زیر **Functional level** مربوط به هریک از **Node** ها را مشاهده کرد:

```
Invoke-Command Node1 {Get-Cluster | fl *}
```

درحقیقت در پاسخ، باید به دنبال سطر **ClusterFuntionalLevel** گشت که مقدار آن، تنها یک عدد است.

برای ارتقا **Cluster Level**، دستور زیر را وارد می کنیم:

```
Update-ClusterFunctionalLevel
```

Cluster Backup:

: First Role Implementation under Clustering

می دانیم که **Windows Server** دارای **Role** های زیادی است، مثلاً **DHCP** ، **DNS** ، **HyperV** ، **FileServer** و ...
حال قصد داریم که یکی از این **Role** ها را جهت پشتیبانی هرچه قوی تر، تحت یک **Cluster** راه اندازی کنیم.

اگر در کنسول **Failover Clustering**، برای اولین بار وارد آبجکت **Role** شویم، می بینیم که خالی است.
برای ایجاد یک **Role**:

- روی آبجکت آن کلیک راست کرده و **Configure Role** را می زنیم.
- همانطور که می بینیم، **Role** های مختلف را به طورواضح لیست کرده است که بتوانیم از هریک از آنها، یک **Cluster** ایجاد کنیم.
- همانطور که می بینیم، اگر در این تب بر روی **Role** ها کلیک کنیم، یک خطای قرمز رنگ، در پایین ظاهر می شود، که نشاندهنده ی موجود نبودن آن **Role** در **Node** های **Cluster** می باشد.

نکته: پس پیشنیاز راه اندازی هریک از **Role** ها تحت **Cluster**، این است که قبل از باز کردن این **Wizard**، آن **Role** موردنظر را بر روی تک تک **Node** های **Cluster** نصب کرده باشیم.

فرض کنید می خواهیم File Server تحت Cluster راه اندازی کنیم:

- گزینه ی **File Server** ران انتخاب کرده و **Next** را می زنیم.
- **File server for general use** را انتخاب می کنیم.
    - کاملاً مشابه راه اندازی **Cluster** اصلی، یک نام و یک **IP** در شبکه ی اصلی **DC** با **Node** ها و ... وارد می کنیم.
    - از آنجایی که از قبل دو دیسک به عنوان **Quorum** و **Data** ایجاد کرده بودیم، در اینجا به سادگی می توان دیسک **Data** را انتخاب کرد، که البته می توان دیسک های بیشتری را نیز اضافه کرد.
    - **Wizard** را به پایان می رسانیم.

- ✓ اگر در **AD** به **OU** مربوط به **Computers** برویم، می بینیم که یک **Object** برای این **Role Cluster** ایجاد شده است.
- ✓ اگر وارد کنسول **DNS** شویم، می بینیم که که **A Record** برای آن ایجاد شده است.
- ✓ یک بار دستور ipconfig /flushdns را وارد می کنیم تا **DNS** گذشته، باعث اختلال نشود!
- ✓ پس در خود کنسول **Failover Clustering** وارد آبجکت **Roles** شده و **Role Cluster** ایجاد شده را انتخاب کنیم و در پایین این کنسول، وارد تب **Shares** شویم، می بینیم که یک **Drive** ایجاد شده است که یک حرف نیز به آن اختصاص داده است. (مثلاً **D**)

جهت دسترسی به این درایو در تمام محیط شبکه، کافی ست با استفاده از نام یکی از **Node** های **Cluster**، آدرس زیر را در **address bar** یک **file explorer** و در ابزار **Run** وارد کنیم:

\\node1\D$
یا
\\node2\D$

نکته: در این حالت **File server for general use** درهر زمان، **File Server** تنها به یک **Node** متصل خواهد بود و تنها از طریق آن **Node** می توان به **File Server** دسترسی داشت، که اگر آن **Node** قطع شود، **File Server** بطور خودکار به یک **Node** موجود دیگر در **Cluster** متصل شده و دوباره اتصال **Start** می شود.

البته اگر **Node** ای که **down** شده است را به عنوان **Owner Node** قطعی **FileServerRole** تعیین کرده باشیم، در اینجا پس از اتصال به **Node** دیگر، ارتباط بطورخودکار **Start** نمی شود.

نکته: برای حذف این **Cluster Role** کافی ست در کنسول **Failover** آن را **delete** کرده و سپس در **AD** آبجکت آن را **delete** کرده و در **DNS** هم اگر **Record** آن بطورخودکار حذف نشده باشد.

- و یا می توانیم Scale-Out File server windows server را انتخاب کنیم.
  - یک نام برای این Role انتخاب می کنیم.
  - Wizard را به پایان می رسانیم.
- به ازای هریک از Node های موجود در Cluster، برای این Role در DNS Server رکورد A ایجاد می کند.
- اگر در AD به OU مربوط به Computers برویم، می بینیم که یک Object برای این Role Cluster ایجاد شده است.
- یک بار دستور ipconfig /flushdns را وارد می کنیم تا DNS گذشته، باعث اختلال نشود!

نکات:

- در این حالت درهر زمان، File Server می تواند به همه ی Node های موجود در Cluster متصل باشد و از طریق همه ی آنها قابل دسترسی باشد. به همین جهت، اگر مثلاً نیاز باشد که یکی از Node ها را جهت تعمیرات و نگهداری، برای مدتی از Cluster جدا کنیم، هیچ خللی در روند کار Cluster و ارتباط با File Server ایجاد نخواهد شد.

- در این روش، وابستگی فرآیند به سخت افزار، به کمترین حالت خود خواهد رسید، چرا که کم و زیاد کردن سخت افزارها، تا حد زیادی هیچ تاثیری بر کارکرد عملیات نرم افزاری نخواهد داشت.

- برای راه اندازی HyperV Server و یا SQL Server از این مدل FileServer Role استفاده می شود.

- جهت اینکه یکی از Node ها را بطور دستی stop یا pause کنیم که از کار بیفتد، به آبجکت Nodes رفته و روی Node موردنظر کلیک راست کرده و Pause و سپس Drain Roles را می زنیم. که در اینصورت، Role های روی آن، بطورخودکار به یک Node دیگر منتقل می شوند.

Directory sharing :

فرض کنید، بخواهیم یک پوشه ی موجود در همان درایو ایجاد شده در File Server را به صورت یکجا اشتراک گذاری کنیم طوری که یک آدرس مجزا و منحصربفرد در شبکه داشته باشد.

- اگر در General File Server باشیم:

- ابتدا یک پوشه در خود آن درایو مربوط به Cluster file server ایجاد می کنیم.
- در کنسول، آبجکت Role را انتخاب کرده و بر روی Role مربوط به File Server ای که ایجاد کرده بودیم، کلیک راست می کنیم.
- Add file Share را می زنیم.
- گزینه ی SMB Share – Quick را انتخاب می کنیم.
- نام Role مربوط به File Server را و در پایین گزینه ی Type a custom path را انتخاب کرده و توسط Browse ، پوشه ی موردنظر در درایو File Server را انتخاب می کنیم.
- یک نام مناسب جهت Shared Name درج می کنیم.
- در تب Configure share setting گزینه ی Enable continuous availability را فعال کرده و Wizard را به پایان می بریم.
- جهت دسترسی به این shared directory:

\\ClusterRoleName\ShareNameOfSharedFolder

نکته: می توان هر از گاهی، جهت refresh کردن بهترین مسیر جهت دسترسی به اطلاعات روی file server Role مربوط به Cluster، روی Role آن کلیک راست کرده و move و سپس Best Possible Node را زد.

- اگر در Scale-Out File server باشیم:

- ابتدا نیاز است که Volume یا Volume های موردنیاز را ایجاد کنیم، که به آن CSV یا **Cluster Shared Volume** گفته می شود. در کنسول Failover، به آبجکت Storage در کادر سمت چپ و به Disks رفته و در کادر میانی بر روی Disk یا Lun ای که به عنوان فضای ذخیره سازی مان ایجاد کرده بودیم، کلیک راست کرده و Add to Cluster Shared Volumes را می زنیم.

نکته: در کادر پایین می بینیم که فرمت این Volume ایجاد شده، CSVFS می باشد، و نه NTFS یا EFS !

- حال به آبجکت Roles رفته و بر روی Role مربوط به File Server ای که ایجاد کرده بودیم، کلیک راست می کنیم.
- Add file Share را می زنیم.
- گزینه ی SMB Share – Applications را (برای HyperV یا SQL و ...) انتخاب می کنیم.
- نام Role مربوط به File Server را و در پایین، گزینه ی Select by volume را انتخاب می کنیم.
- یک نام مناسب جهت Shared Name درج می کنیم.
- در تب Configure share setting گزینه ی Enable continuous availability باید بطورپیشفرض فعال باشد.
- Wizard را به پایان می بریم.
- جهت دسترسی به این shared directory:

\\ClusterRoleName\ShareNameOfSharedFolder

Node Priorities to own a Role :

فرض کنید چندین Node در Cluster داریم که دو عدد از آنها قدرت بالاتری دارند، پس می خواهیم که آن دو را در اولویت بالاتری جهت دسترسی دادن کاربر به Cluster قرار دهیم. پس بر روی Role ای که ایجاد کرده بودیم، کلیک راست کرده و Properties.

- در تب General، فقط آن Node های موردنظر را تیک می زنیم. البته در صورت اینکه هردوی آن دو Node دچار ایراد شوند، خود Cluster به طور خودکار، دسترسی به Cluster به Node های دیگر خواهد داد.
- در تب Failover همین پنجره، برای maximum failures می توان عدد **تعداد Node ها منهای یک** را برای 6 ساعت درج کرد.
- همچنین در پایین تب Failover می توان تعیین کرد که اگر یک Node برای مدتی دچار مشکل شد و دوباره به Cluster برگشت، به چه شکل و چند مدت بعد، نقش های owner ای که داشته بوده است را دوباره دریافت کند!
- جهت تنظیمات بیشتر بر روی Owner های یک Role، آن را انتخاب کرده و در پایین کنسول، وارد تب Resources شده و وارد Properties گزینه ی File Server شده و به تب Advanced Policies می رویم.

Dependencies:

درحقیقت هر Cluster Role ای که راه اندازی می کنیم، یک سری وابستگی ها (Dependency) دارد که اگر یکی از آنها دچار ایراد یا خرابی شود، فرآیند و کارآیی Role ، قطع خواهد شد.

- برای مشاهده ی این Dependency های مربوط به یک Role، روی آن کلیک راست کرده و از more Actions گزینه ی Show Dependency Report را می زنیم.
- برای اضافه کردن یا حذف این Dependency ها، Role موردنظر را انتخاب کرده و در پایین کنسول، وارد تب Resources شده و وارد Properties مربوط به گزینه ی File Server شده و به تب Dependencies می رویم.

Improve the Cluster speed:

ابتدا در PowerShell توسط دستور زیر مشخصات Cluster را فراخوانی می کنیم:

```
Get-Cluster -Name CLUSTERNAME | fl*
```

همانطور که در نتیجه می بینیم، مقداری وجود دارد به نام BlockCacheSize که مقدار آن بطورپیشفرض صفر است.

پس بهتر است که مقداری را به آن اختصاص دهیم، بطور مثال 1GB :

```
(Get-Cluster -Name CLUSTERNAME).BlockCacheSize = 1024
```

حال اگر دوباره مشخصات Cluster را فراخوانی کنیم، می بینیم که مقدار آن تغییر کرده است، که این قابلیت، مفید واقع خواهد شد.

:HyperV Clustering

ابتدا باید **Clustering** را مطابق تنظیمات گذشته، راه اندازی کنیم، تا قبل از راه اندازی **File Server Role**.

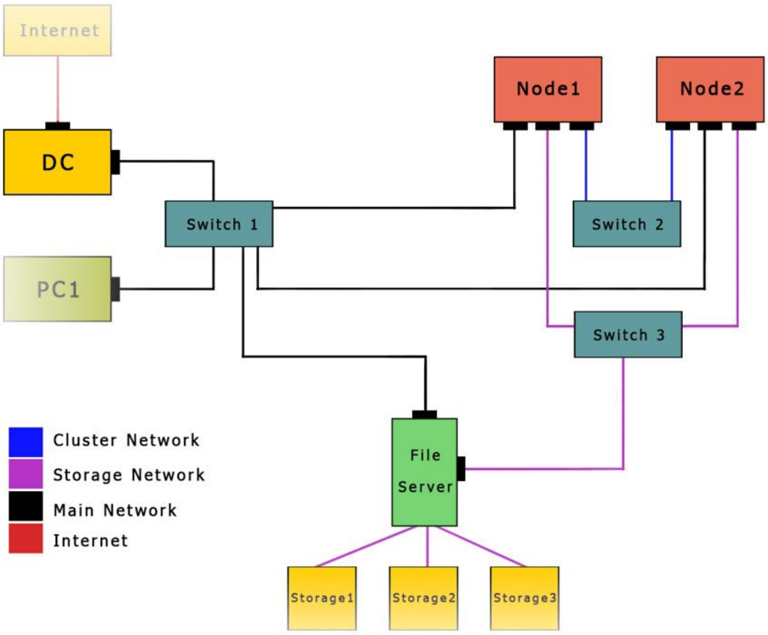
حال باید **Role** مربوط به **HyperV** را بر روی تک تک **Node** های عضو **Cluster** و همچنین بر روی **DC** یا سیستم درنظرگرفته شده برای آن، نصب کرده باشیم، که البته پیشنیاز آن هم، فعال کردن قابلیت مجازی سازی در تنظیمات صفحه ی **UEFI** سیستم ها می باشد:

```
Invoke-Command Node1,Node2 {Install-WindowsFeature Hyper-v}
```

و پس از نصب هم لازم است که یکبار سیستم ها را یکبار **Restart** کنیم.

در **Active Directory** قابلیت **delegation** (یا محول کردن مدیریتِ) **Node** ها را برای سیستمی که قرار است **HyperV Server** باشد، و همچنین **Delegation** مربوط به **HyperV Server** را برای تک تک **Node** ها معرفی می کنیم:

- وارد **AD** و **Properties** مربوط به **HP-Server** شده و به تب **Delegation** می رویم.
- **Trust this computer for delegation to…** و سپس **Use any authentication protocol** را فعال می کنیم.
- دکمه ی **Add** را زده و تک تک **Node** ها را **Add** کرده و **OK**.
- حال وارد **Properties** مربوط به هریک از **Node** ها شده و به همین شکل آبجکت **HP-Server** را اضافه می کنیم.



- **HyperV management** را نصب می کنیم.

- در اینجا، این قابلیت مدیریت **HyperV** را بر روی خود **DC** نصب می کنیم.
- وارد **Wizard** مربوط به **Add Roles and Features** می شویم.
- در تب **select features** گزینه ی **Remote Server Administration Tools** را و سپس **Role Administration Tools** را و بعد گزینه ی **Hyper-V Management Tools** را همراه با زیرگزینه های آن فعال می کنیم و **Wizard** را به پایان می بریم.
- سیستم را یکبار **Restart** می کنیم.
- کنسول **Hyper-V Manager** را باز کرده و بر روی آبجکت آن در کادر سمت چپ، کلیک راست کرده و **Connect Server** را زده و با درج نام های کامل **Node** های یک و دو، آنها را فراخوانی می کنیم.
- برای هریک از این **Node** ها، یک **Switch** از نوع **external** ایجاد می کنیم.

نکته: حال اگر به HyperV Settings و بخش Live Migration هریک از دو Node ها برویم، می بینیم که هم enable شده است و هم دو آدرس IP مربوط به Node ها را بطورخودکار تعریف کرده است.

- از زیرگزینه های **Live Migration**، به **Advanced Features** رفته و گزینه ی **User Kerberos** را فعال می کنیم. (برای هردو)

- **HyperV Clustering Role را با ایجاد VM راه اندازی می کنیم.**

- در همان سیستم DC (یا هرسیستمی که کنسول Failover Clustering راه اندازی شده است) آن را انجام می دهیم.
- بر روی آبجکت Roles کلیک راست کرده و Virtual Machines و سپس New Virtual Machine را می زنیم.
- یکی از Node ها را انتخاب می کنیم و وارد wizard می شویم.
- یک نام برای VM درج کرده و توسط گزینه ی Location، یک مکان جهت ذخیره سازیِ آن در خود دیسک (ایجاد شده برای Cluster) تعریف می کنیم.
- Generation 2 را انتخاب و پس از درج مقداری برای Ram، گزینه ی Use Dynamic Memory را فعال می کنیم.
- برای گزینه ی Connection، گزینه ی سوییچ مجازی external ای که ایجاد کردیم را می زنیم.
- فایل ISO مربوط به نصب ویندوز را برای آن انتخاب می کنیم و Wizard را به پایان می رسانیم.
- روی VM کلیک راست و Start می کنیم و نصب ویندوز را به پایان می رسانیم.

در کنسول Failover، یک VM دیگر ایجاد می کنیم، اما آن را به Node دیگر اختصاص می دهیم. (Owner Node باید Node دیگر باشد.)

Migration:

بطورمثال می توان به سادگی یک VM را از Node1 به Node2 جابجا کرد.

به سه شکل می توان VM ها را جابجا یا منتقل کرد:

- Live Migration : هیچ خللی در روند کاری VM ایجاد نمی شود.
- Quick Migration: VM را نگه می دارد یا pause می کند و سپس آن را به Node دیگر منتقل کرده و روشن می کند.
- Virtual Machine Storage: تنها virtual Disk مربوط به VM را منتقل می کند.

✓ برای انجام هریک از دو حالت اول بطورخودکار، می توان روی VM موردنظر در کنسول Failover کلیک راست کرده و Move را زده و هریک را انتخاب کرده و از گزینه های آن، Best Possible Node را زد تا انجام گیرد.

✓ برای انجام حالت سوم، از زیرگزینه های Move، گزینه ی Virtual Machine Storage را می زنیم.

می بینیم که مشخصات کامل آن VM را می توان جابجا کرد، مثلاً برای جابجا کردن V-Disk، آن را انتخاب کرده و دکمه ی Copy را زده و در نوار پایین، گزینه ی Add Share را می زنیم و یک آدرس تحت شبکه ی موردنظر جهت انتقال را وارد می کنیم.

Balancing :

توسط این قابلیت، می توان VM ها را بر اساس میزان منابعی که Node ها دارند، روی آنها تقسیم کنیم.

برای فعال کردن این قابلیت:

➢ در کادر سمت چپ کنسول Failover بر روی آبجکت DC کلیک راست کرده و Properties را می زنیم.

➢ وارد تب Balancer شده و Enable Automatic Balancing را فعال می کنیم.

➢ اگر گزینه ی Always load balance را بزنیم، هر 30 دقیقه یکبار balancing را با توجه به میزان aggressiveness چک می کند.

➢ میزان aggressiveness به صورت زیر است:

High : 80%

Medium : 70%

Low : 60%

که به این صورت عمل خواهد کرد که مثلاً اگر میزان اشغال منابع در Node به درصد تعیین شده برسد، VM یا VM ها را به یک Node دیگر migrate بدهد؛ از نوع Live migration.

➢ اگر گزینه ی Load balance to a node when it joins را بزنیم، تنها زمانی که یک node جدید به Cluster اضافه می کنیم، این عملیات balancing را انجام می دهد و VM ها را بین Node ها پخش می کند.

نکات:

- برای اینکه در کنسول Failover، جهت مدیریت یک VM، فوری به کنسول HyperV آن VM برویم، روی آن VM کلیک راست کرده و Manage را می زنیم.
- فرض کنید ارتباط یک Cluster Node با شبکه قطع شود! راه حلی که در Clustering وجود دارد این است که در این حالت، VM های موجود در آن Node را به یک Node دیگر که همچنان ارتباط با شبکه دارد، منتقل کند.
  این قابلیت را برای تک تک VM ها باید به صورت جداگانه فعال یا غیرفعال کرد، به این صورت که:
  - روی آن VM در کنسول Failover کلیک راست کرده و Settings را می زنیم.
  - به گزینه ی Network Adapter و سپس به Advanced features می رویم.
  - گزینه ی Protected Network را فعال می کنیم.
- فرض کنید بخواهیم یک VM، که در آن فقط و فقط یک Service ارایه می شود (single service)، در صورت down شدن آن Service، بطورخودکار Restart شود، تا بلکه آن Service دوباره Run شود.
  - پس در کنسول Failover برروی VM موردنظر کلیک راست کرده و More Actions را و سپس Configure Monitoring را می زنیم.

نکته: اگر خطا داد یا صفحه ی سپید باز شد، وارد VM شده و Time Zone و IP address را تنظیم و Firewall را off می کنیم.

  - سرویس موردنظر را تیک زده و OK می کنیم.

نکته: درحقیقت اگر وارد کنسول Services مربوط به Node ای که owner مربوط به VM موردنظر است شویم، و وارد Properties یک Service و تب Recovery شویم، می بینیم که برای دو Failure اول، یک عکس العمل تنظیم شده است (Restart the Service)، اما برای سومین، Take no action.

پس در Node موردنظر که VM روی آن قرار دارد، این take no action به Cluster اجازه ی دخالت می دهد.

: Guest clustering

ما می توانیم چند VM ای که به عنوان Role در کنسول Failover clustering ایجاد ایجاد کرده ایم را به عنوان Node های یک Cluster جدید تنظیم کنیم.

پیشنیازها:

- ابتدا نیاز است که Cluster اصلی را همراه با یک Scale-Out File server و یک CSV Volume راه اندازی کرده باشیم.
- VM ها از طریق یک virtual external SW به Domain متصل، و عضو Active directory باشند (Join باشند).

- **Feature مربوط به Failover clustering را بر روی Node ها راه اندازی می کنیم:**

```
Invoke-Command Node1,Node2 {Install-WindowsFeature Failover-Clustering}
```

- **یک Share Storage برای آنها ایجاد می کنیم:**
  - روی آبجکت Roles کلیک راست کرده و Virtual Machines و سپس New Hard Disk را می زنیم.
  - یکی از Node های غیرمجازی را انتخاب می کنیم.
  - VHD Set را می زنیم.
  - Dynamically expanding را می زنیم.
  - یک نام دلخواه برای این V-Disk درج می کنیم و Location آن را، جایی در CSV Volume تعیین می کنیم.
  - یک حجم دلخواه فعلاً تعیین می کنیم (مثلاً 120 GB) و finish.
  - وارد Properties تک تک VM ها شده و به بخش SCSI Controller رفته و Shared Drive را انتخاب و Add را می زنیم. گزینه ی Browse را زده و فایل VHD-Set ای که ایجاد کردیم را اضافه کرده و پنجره ی Properties را Ok می کنیم.

- **VHD Set را تنظیم می کنیم.**
  - می توان با ورود به یکی از VM ها این کار را انجام داد و یا اینکه وارد Server manager مربوط به DC شد.
  - در Server manager توسط manage و Add Servers یکی از VM ها را اضافه می کنیم.
  - به بخش File and storage services و سپس به Disks رفته و در کادر مقابل، گزینه ی VM موردنظر را انتخاب می کنیم.
  - از زیرمجموعه های آن، بر روی Disk ای که به صورت offline قرار دارد کلیک راست کرده و Bring online را می زنیم.
  - دوباره روی آن کلیک راست کرده و Initialize را می زنیم.
  - دوباره روی آن کلیک راست کرده و اینبار New Volume را می زنیم.
  - Wizard را تا پایان پیش می رویم.

- **Guest Cluster را ایجاد می کنیم.**
  - در کنسول Failover Cluster در کادر سمت چپ، بر روی اولین آبجکت، یعنی Failover Cluster Manager کلیک راست کرده و Create Cluster را زده و در تب Select Servers ، هریک از VM ها را اضافه می کنیم.
  - گزینه ی Yes را برای Validation Warning انتخاب می کنیم.
  - Run all Tests را می زنیم.
  - پس از انجام Validation، برای Cluster Name، یک نام درج می کنیم.
  - یک IP در رنج شبکه ی اصلی درج می کنیم.
  - Wizard را به پایان می رسانیم.

- **یک Quorum ایجاد می کنیم.**
  - در اینجا یک SMB Share را ایجاد می کنیم که می توان به File Server رفت و در آنجا، اینکار را کرد.
  - پس وارد سیستم file Server و server manager آن شده و به file and storage services رفته و از دکمه ی TASKS گزینه ی New Share را زده و SMB Share-Quick را انتخاب می کنیم.
  - یکی از drive ها را انتخاب کرده و یک پوشه ی مخصوص witness برای آن ایجاد می کنیم.
  - یک Share name برای این Witness درج می کنیم.

  - حال به سیستم DC و به کنسول Failover Cluster برگشته و روی آبجکت این Guest Cluster کلیک راست می کنیم.
  - گزینه ی More Actions و سپس Configure Cluster Quorum settings را می زنیم.
  - در ویزارد باز شده، گزینه ی Select the quorum witness را می زنیم.
  - گزینه ی Configure a file share witness را انتخاب می کنیم.
  - توسط Browse و سپس Browse، ابتدا سیستم File Server را فراخوانی می کنیم.
  - پوشه ای که SMB Share کردیم را انتخاب می کنیم.
  - ویزارد را به پایان می رسانیم.

Storage Space Direct (S2D):

در این فرآیند، می توان از تمامی Storage های فیزیکی که بطور local به هریک از Server های موجود در شبکه متصل شده اند، Pool Storage تهیه کرد و از آن Pool، Virtual Disk هایی را راه اندازی کرد.

- **به این روش، Locally-Attached software defined storage هم گفته می شود.**
- **این روش باعث می شود که نیاز به SAN یا NAS های فیزیکی و قدرتمند از بین برود.**
- **این روش تا شانزده Server و تا چهارصد Drive را پشتیبانی می کند.**
- **همه ی درایوهای با درگاه های SAS، SATA، NVMe، HDD، SSD را پشتیبانی می کند.**

این فرآیند به دو شکل متفاوت قابل پیاده سازی است:

- **Disaggregated Cluster (Converged):**

در این روش، دو Cluster خواهیم داشت:

  - **Storage Cluster و HyperV Cluster که بطورجداگانه ایجاد شده و در پایان به یکدیگر متصل می شوند.**
  - **هردو Cluster قابلیت Scale out یا بسط و اضافه کردن Server ها یا Node ها را خواهند داشت.**

- **Hyper-Converged Cluster:**

در این روش، هم HyperV Cluster یا هر Role دیگر، به همراه Storage Cluster در یک مجموعه Cluster خواهند بود.

:(NLB) Network Load Balancing

در دنیای امروز، افراد به Service ها به صورت آنی نیاز دارند.
سازمان ها از تکنولوژی ها و راه حل های متفاوتی برای ایجاد redundancy و High Availability استفاده می کنند.
NLB یکی از معروفترین ویژگی هایی ست که در این زمینه استفاده می شود.

Network Load Balancing یا NLB یکی از قابلیت های Windows Server است که این امکان را می دهد که مجموعه ای از Server ها را که یک سرویس یکسان ارائه می دهند را در قالب یک گروه در کنار هم قرار دهیم.
اما برای کاربر، همه ی این Server ها به عنوان یک Server دیده می شوند و کاربر از مشاهده ی همه ی آنها ناتوان است.

تصور کنید 10 عدد Server با 10 آدرس IP متفاوت داریم و همه ی آنها با استفاده از سرویس Network Load Balancing در Windows Server به شکل یک گروه در آمده اند.
تمام این 10 عدد Server برای کاربر، فقط با یک آدرس IP دیده می شوند.و این آدرس IP مربوط به گروهی ست که در آن قرار گرفته اند.
به این گروه NLB Cluster یا خوشه گفته می شود.

هر کدام از Server هایی که به NLB Cluster اضافه می شوند، به عنوان یک Host یا Node شناخته می شوند.
هدف از راه اندازی سرویس NLB، بالا بردن Availability و مقیاس پذیری یا Scalability مربوط به سرویس هایی است که روی Node های یک NLB Cluster قرار گرفته اند.

- به اصطلاح، به سیستمی که سرویس NLB را برای آن فعال کرده ایم و این عملیات را برعهده گرفته است، Load Balancer می گویند.
- سرویس NLB درLoad balancer، درخواست های Client ها را دریافت کرده و آنها را میان Node های Cluster توزیع می کند.
- اگر Load Balancer به صورت نرم افزاری (مثل سرویس ویندوز Server) باشد، به آن SLB یا Software Load Balancer گفته می شود.

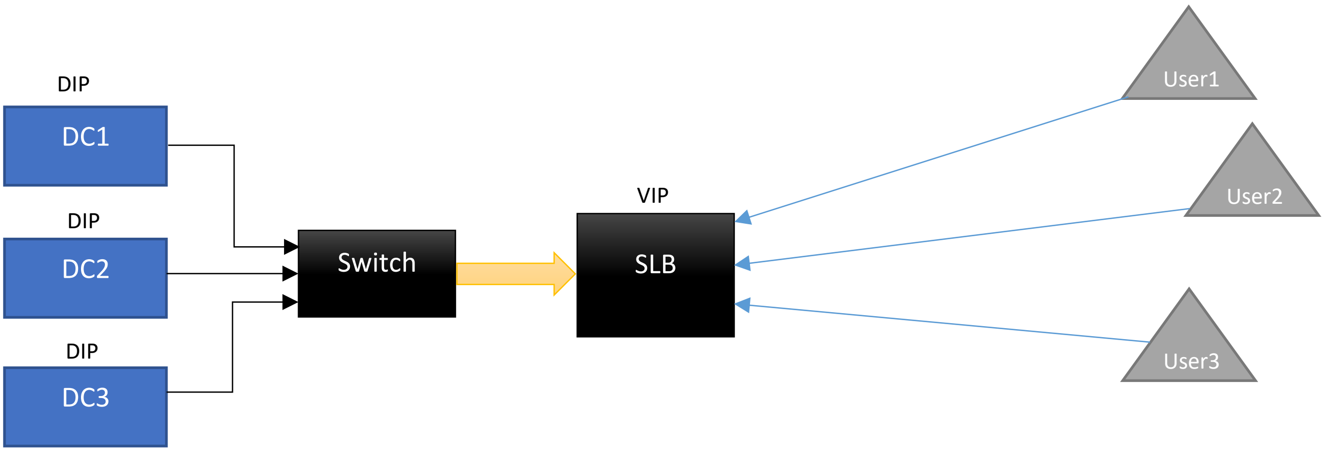
بیشترین استفاده ای که از NLB Cluster می شود، در وب سایت ها و نرم افزارهای کاربردی تحت وبی است که در سطح سازمان استفاده می شوند. ما در چنین حالتی یک Web Farm ایجاد می کنیم.

همچنین می توانیم Remote Desktop Farm یا VPN Server Farm و یا حتی Proxy Server Farm هم با استفاده از NLB ایجاد کنیم.

- چیزی که NLB برای بالا بردن Availability به ما ارائه می دهد این است که با استفاده از شناسایی Server های مشکل دار، دیگر درخواستی را به سمت آنها ارسال نمی کند. به این شکل هیچ کلاینتی متوجه بروز مشکل در Server ها نمی شود و سرویس دهی همچنان ادامه پیدا می کند.
- یکی از مزایای استفاده از NLB این است که در هر زمان، گروهی از Server ها، درخواست های کاربران را مدیریت و پاسخگویی می کنند.
  مثلاً با بالا رفتن تعداد درخواست های کاربران به یک Web Server، می توان یک Server جدید را به مجموعه ی NLB Cluster اضافه کرد و Load کاری را بین Server های بیشتری تقسیم کرد.
- نکته ی مهم این است که درخواست های هر Client فقط بصورت مستقیم برای یکی از Node های مستقر در NLB Cluster ارسال می شوند.
- این یعنی Client فقط و فقط از قدرت پردازشی و منابع ذخیره سازیِ یکی از Server های موجود در NLB Cluster استفاده خواهد کرد و Server های دیگر، درگیر پردازش این درخواست نخواهند شد.

- در یک NLB Cluster هر کدام از Node ها بصورت مستقل کار می کنند و هیچ دسترسی به منابع موجود بر روی سرورهای دیگر ندارند و نمی توانند بر روی سرورهای دیگر تغییر ایجاد کنند.
- ما نمی توانیم از NLB برای Stateful Application ها استفاده کنیم. مثلاً خود Web Server که دارای پیچیدگی و پایگاه داده ی خاصی نیست، می تواند توسط NLB سرویس دهی شود.
- می توان Database Server ها را در یک NLB قرار داد، چون هر یک از Client ها که درخواستی جهت بروزرسانیِ پایگاه داده ای داشته باشد، ممکن است ایجاد تداخل کند.

- به آدرس IP هریک از Server های متصل به NLB ، DIP یا Dynamic IP گفته می شود.
- اما هریک از User ها برای دسترسی به سرویس یا داده های مورد نیازشان که درون هریک از Server ها می تواند باشد، فقط به IP مخصوص NLB دسترسی دارند که به آن VIP یا Virtual IP گفته می شود.



- NLB/SLB Cluster می تواند تا سی و دو HOST را شامل شود.
- نیازی نیست که Host ها دارای سخت افزار مشابه باشند.
- همه ی Host ها باید به یک IP Address Subnet متصل باشند (در یک شبکه ی IP Address باشند.)
- سرعت شبکه باید آنقدر بالا بوده و میزان تاخیر چنان کم باشد که عملیات convergence سریع انجام شود.
- نیازی نیست که همه ی Host ها در یک Datacenter قرار داشته باشند ولی اگر فاصله ی فیزیکی زیاد باشد، ممکن است باعث drop شدن Host از NLB Cluster شود.

- نیازهای نرم افزاری:
  - بهتر است همه ی Host ها از Windows با Version و Edition مشابه استفاده کنند.
  - همه ی Host ها باید دارای Static IP Address بوده و سرویس DHCP Client روی آنها Disable باشد.
  - باید یک User Account مشابه (از نظر first name و last name و logon name و password) روی تک تک Host ها وجود داشته باشد و در هر کدام از آنها عضو گروه local administrators نیز باشد.
  - این Account مورد استفاده ی NLB Cluster قرار می گیرد.

- در شبکه هایی که بیش از یک سایت فیزیکی وجود دارد، بهترین کار این است که در هر سایت یک NLB Cluster مخصوص آن سایت وجود داشته باشد و آنگاه از تکنیک دیگری برای توزیع Client Query ها میان Server ها استفاده شود.
- مثلاً برای این کار می توان از DNS Round Robin استفاده کرد، که DNS Server ها را قادر می سازد که درخواستهای Client های هر سایت، به NLB Cluster همان سایت هدایت شود.

- روش ارتباط Client ها با Server ها برای دسترسی به Service مورد نظرشان، به این شکل است که:
  - درخواست یک Client به SLB Server یا NLB Server وارد شده و او هم درخواست را به Server موردنظر ارسال می کند.
  - Server پس از دریافت درخواست و بررسیِ آن، پاسخ آن درخواست را بطور مستقیم به Client موردنظر ارسال می کند.

- اگر Client در داخل شبکه ی LAN باشد، به این ارتباطش با Server ها، East-West LB گفته می شود.
- اگر Client از خارج از شبکه ی LAN باشد، به این ارتباطش با Server ها، North-South LB گفته می شود.

مفهومی در NLB Cluster وجود دارد بنام Operation Mode که شامل سه گزینه است:

- Unicast:
  - در این حالت هر Server باید دارای 2 NIC باشد، یکی برای اتصال به NLB که به آن NLB NIC گفته می شود و یکی برای اتصال به Server دیگر؛ جهت اینکه از active یا down بودن Node های دیگر مطلع شوند.
  - حالت unicast باعث می شود که MAC Address متعلق به Cluster در تک تک Host ها، جاگیزین MAC Address مربوط به آن کارت شبکه ی آنها شود.
  - پس در این حالت همه Server ها دارای MAC Address مشابهی خواهند شد و به این صورت خطر روی دادن Port Flooding بر روی Switch کمتر می شود.
- Multicast:
  - NIC هر Server دارای یک MAC Address دوم می شود. پس هر NIC دارای دو MAC Address خواهد بود.
  - پس هیچکدام از Server ها نیازی به داشتن یک NIC دوم نخواهد بود.
  - احتمال بروز حمله ی Port Flooding وجود دارد، اما کمتر از حالت Unicast.
- IGMP multicast:
  - این حالت به جهت برطرف کردن احتمال Port Flooding در حالت Multicast ایجاد شد.
  - در این حالت نیاز به config کردن متناسب Switch یا Router مرتبط با IGMP خواهد بود.

- پس NIC هایی که روی Server ها برای NLB استفاده می شوند، باید دارای Operation Mode مشابه باشند!
- معمولا توصیه می شود که برای Operation Mode از گزینه ی IGMP multicast استفاده شود، مگر اینکه شبکه قادر به پشتیبانی از ارتباطات Multicast نباشد!

NLB دارای سه Filtering mode می باشد:

- None یا Disable، که NLB را کاملاً غیرفعال می کند.

برای درخواست ها و Server ها و یا Website هایی که dynamic و یا session base هستند مثل تراکنش های مالی و ...، هیچگاه NLB را در حالت None قرار نمی دهیم. اما برای وبسایت های Static و یا video streaming می توان از این mode استفاده کرد، به همین جهت نوع پروتکل را UDP و یا هم UDP هم TCP (both) تعیین می کنیم.

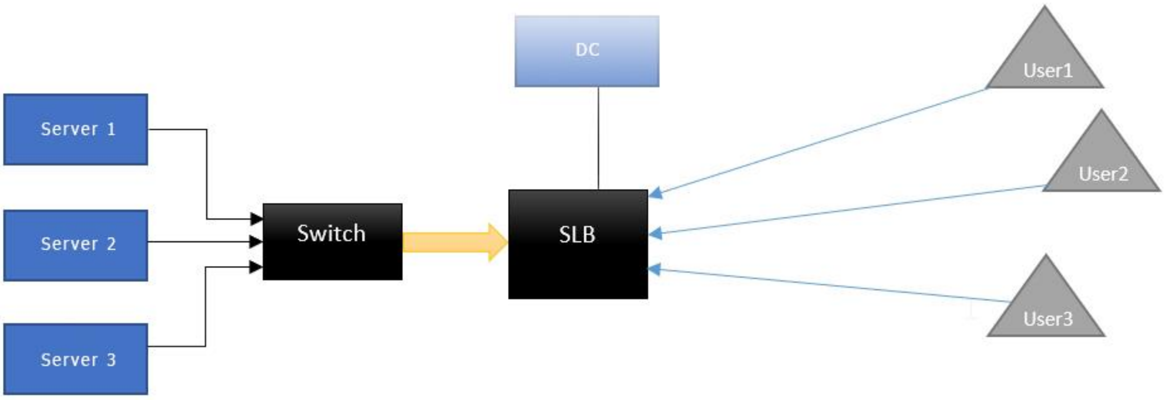
- Single: فقط با یک Server ارتباط برقرار می کند که مشابه failover clustering خواهد بود؛ طوری که اگر آن Server از کار بیفتد، NLB بطورخودکار ارتباط را به Server بعدی منتقل می کند. برای وبسایت های Dynamic گزینه ی مناسبی است.
- Multi: این حالت، خودش به سه شکل قابل پیاده سازی است:
  - None: مشابه با round robin عمل می کند. به این شکل که وقتی NLB درخواست یک Client را به یک Server ارسال می کند؛ درخواست بعدی که همان Client ارسال می کند را به یک Server دیگر ارسال می کند.
  - Single: در این حالت هر Server ای که جهت رسیدگی به درخواست یک تخصیص داده شود، در دفعات بعدی هم همان Server اختصاص خواهد یافت. اما اینکه در اولین بار کدام Server اختصاص داده می شود، به work load آنها مرتبط است.
  - Network: تنها درخواست Client هایی که آدرس IP آنها در Class C قرار دارد را به شکل تصادفی میان Server ها پخش می کند.

برای Stop کردن هریک از Server ها یا Cluster های متصل به NLB ، دو گزینه ی زیر وجود دارند:

- **Stop Action: بلافاصله تمامی Session ها و ارتباطهای در حال برقراری و یا در حال اتصال، قطع شده، و خاموش می شود.**
- **Drain-Stop: بلافاصله راه را برای دریافت درخواست Session های جدید block می کند، اما صبر می کند تا Session هایی که در حال حاضر برقرار هستند، به اتمام برسند، و سپس Server را قطع و خاموش می کند.**

:NLB Implementation

در اینجا NLB را در mode از نوع **multi** راه اندازی می کنیم.
در اینجا می خواهیم یک Web Server را بر روی سه Server راه اندازی کنیم، طوری که balancing میان آنها برقرار باشد.



نکته: در حقیقت، با توجه به اینکه نقش Web Server میان آن سه Server تقسیم می شود، پس نیازی نخواهد بود که برای SLB هم یک سیستم فیزیکی جداگانه در نظر بگیریم، تنها کافی ست NLB Cluster را بر روی خود DC نصب و مدیریت کنیم.

- **Feature مربوط به NLB را بر روی اعضای این NLB Cluster (Server ها) نصب می کنیم.**

اما قابلیت RSAT-NLB را نیز جهت مدیریت از راه دور، بر روی آنها نصب می کنیم.
پس در سیستم DC وارد PowerShell می شویم:

```
icm Server-1,Server-2,Server-3 {Install-WindowsFeature NLB,RSAT-NLB,Web-Server}
```

سپس وارد تنظیمات Adapter کارت شبکه ی هریک از Server ها شده و تیک گزینه ی Network Load Balancing را می زنیم، وگرنه کارت شبکه ی آنها در ویزارد ایجاد کردنِ Cluster نمایش داده نمی شوند.

- **Feature مربوط به NLB را بر روی NLB Server یا همان SLB (که احتمالاً همان DC خواهد بود) نصب می کنیم.**

- اما قابلیت RSAT-NLB را نیز جهت مدیریت از راه دور، بر روی آنها نصب می کنیم.

از طریق PowerShell:

```
New-NlbCluster -InterfaceName "Ethernet0" -OperationMode Multicast
-ClusterPrimaryIP 192.168.1.115 -ClusterName NLB.payamavar.local -Verbose
```

از طریق GUI:

- در Server manager و Tools گزینه ی Network load Balancing Manager را باز می کنیم.
- در کادر سمت چپ، بر روی آبجکت ..Network load Balancing Cl کلیک راست کرده و New Cluster را می زنیم.
- در کادر Host نام Server اول را وارد کرده و Connect را می زنیم و Next.
- در تب Cluster IP addresses باید آدرس مجازی را برای این Cluster تعریف کنیم. Add را زده و آدرسی در رنج شبکه ی Domain را به آن نسبت می دهیم، مثلاً: **192.168.1.115** همراه subnet address کلاس C و OK می کنیم.
- در تب .Cluster IP Config برای Full Internet name یک نام کلی برای دسترسی به این Cluster تعیین می کنیم. {در DNS Server نیز به عنوان یک A Record این Cluster ثبت می کنیم.: مثلاً **NLB.payamavar.local** }
- Multicast را انتخاب می کنیم.
- و در تب آخر که باید finish را بزنیم، Rule ای که ایجاد شده است، در بالا دیده می شود، آن را انتخاب کرده و Edit را می زنیم.
- چون می خواهیم Web Server را تحت این NLB راه اندازی کنیم، هر دو مقدار From و To را بر روی 80 قرار می دهیم.
- TCP و سپس Multicast و Single را انتخاب و OK می کنیم.
- چند لحظه طول می کشد تا این Server به عنوان NLB Node به این NLB Cluster اضافه شده و نشانه ی آن سبز شود.

حال به همین شکل، Server های دوم و سوم را نیز به NLB Cluster اضافه می کنیم.

نکات:

- یک روش جهت تست اینکه NLB به درستی کار می کند، این است که از درون SLB دستور زیر را وارد کنیم:

```
icm Server1,server2,server3 {"It's <b>$env:ComputerName</b> ." > C:\inetpub\wwwroot\iisstart.htm}
```

این دستور، متن درون براکت را در فایل تست IIS جایگزین می کند، که نام سیستمی که پاسخ می دهد را نشان می دهد!
حال از سیستم های مختلف نام یا IP مربوط به NLB Cluster را در Browser فرا می خوانیم؛ که باید در هر سیستم، نام Node های متفاوت Cluster درج شود.

- برای تغییر VIP یا operation mode و یا filtering mode کافی ست در همین کنسول، بر روی آبجکت Cluster کلیک راست کرده و Cluster properties را بزنیم.

- برای اینکه وزن یا بار کاری یکی از Node های این Cluster را کم یا زیاد کنیم، روی آن آبجکت آن Server کلیک راست کرده و Host properties را زده و به تب Port Rules می رویم و Rule را انتخاب کرده و Edit را زده و گزینه ی Equal را غیرفعال کرده و مقدار Load weight را با عدد مقابلش تنظیم می کنیم.

- اگر تغییری در تنظیمات ایجاد کردیم و نشانه ی node ها یا خود Cluster زردرنگ شد، کافی ست روی نشانه ی خود Cluster کلیک راست کرده و refresh را بزنیم.

- برای Stop کردن یکی از Node ها، کافی ست روی نشانه (آبجکت) آن، کلیک راست کرده و Control host و سپس Stop را بزنیم.
- برای مشاهده ی مشخصات همه ی Node ها از طریق PowerShell، وارد یکی از node ها شده و دستور زیر را وارد می کنیم:

```
Get-NlbClusterNode | fl *
```

SDN (Software Defined Networking) :

[شبکه های نرم افزار محور]

تکنولوژی **SDN** برای ساده سازی کنترل شبکه های پیچیده، پدید آمد.
برای اینکه با شبکه های **SDN** آشنا شویم، لازم است که ابتدا با شبکه های معمولی یا غیر **SDN** آشنا باشیم.
در شبکه های معمولی/سنتی، کلیه ی عملیات و وظایف در هر **Network Device** ، در سه لایه، دسته بندی می شوند:

- **Data Plane**: به آن، Forwarding Plane هم گفته می شود.
- **Control Plane**
- **Management Plane**

Data Plane:

وقتی یک **Packet** به یک **Network Device** مثل **Switch** می رسد، بر طبق لایه ی **Data Plane**، عملیات زیر روی آن اعمال می شوند:

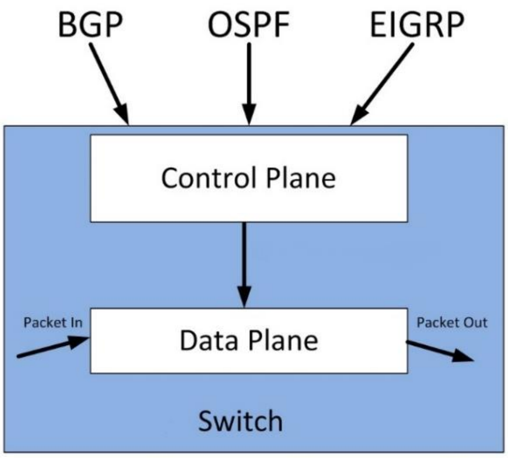
- **De-encapsulation** (تجزیه و تحلیل محتویات) و **Re-encapsulation** (دوباره بسته بندی و کپسوله کردن)
- در دستگاه های لایه دویی، جهت بررسی **MAC address** و هدایت **Packet**، به **Mac address table** مراجعه خواهد شد.
- در دستگاه های لایه سه ای، جهت بررسی **IP address** و هدایت **Packet**، به **Routing table** مراجعه خواهد شد.
- اگر قرار بر ارسال **Packet** در بستر **VPN** باشد، **Packet** رمزنگاری و یک **Header** جدید به آن اضافه می شود.
- در صورت وجود **Vlan tag** بر روی **Packet**، تگ **.1Q** خوانده و بررسی و تغییرات لازم، اعمال می شوند.
- انجام عملیات **NAT** بر روی **Packet** (که بطورمعمول لازم است)
- درصورت وجود **ACL** (هم روی Source interface، هم روی Destination interface) خوانده و بررسی و تغییرات لازم، اعمال می شوند.

Control Plane:

درحقیقت، پردازش و تصمیمگیری های مهم در مورد **Packet** ها، بر عهده ی **Control Plane** است.
قطعه ی **CPU** در **Network Device** ها، هسته ی اصلی لایه ی **Control Plane** در آنهاست.

وقتی یک **Packet** به یک **Network Device** مثل **Switch** می رسد، بر طبق لایه ی **Control Plane**، عملیات زیر روی آن اعمال می شوند:

- بررسی اینکه یک **Packet** به چه شکل و از کدام **Interface** وارد **Network Device** شده است، و باید از کدام **Interface** خارج شود.
- اعمال و پیاده سازی و مدیریت پروتکل ARP برای آدرسدهی بر پایه ی **IPv4**
- اعمال و پیاده سازی و مدیریت پروتکل NDP برای آدرسدهی بر پایه ی **IPv6**
- پیاده سازی عملیات **MAC learning** در **Switch** ها
- پردازش و اعمال پروتکل **STP**
- پیاده سازی و مدیریت **Routing Protocol** ها مثل: OSPF ، EIGRP و ... .



:Management Plane

این لایه شامل پروتکل هایی می شود که به کاربر اجازه ی مدیریت Network Device را می دهد.

پروتکل های معروف در Management Plane:

- SSH
- Telnet
- SNMP
- Syslog

درحقیقت، اگر یکی از دو لایه ی Data Plane و Control Plane دچار مشکل شوند، شبکه دچار اختلال خواهد شد؛ اما اگر لایه ی Management Plane دچار مشکل شود، در کارکرد شبکه، اختلالی ایجاد نخواهد شد.

از وظایف معروف Management Plane:

- **هدایت، اجرا و مدیریت Session های SSH و Telnet**

:SDN Controller

در معماری SDN لایه های کنترل و داده (Control Plane | Data Plane) از یکدیگر جدا هستند.
درحقیقت در شبکه های SDN، قسمت Control Plane روی Network Device ها حذف خواهد شد، چون تمامی وظایف Control Plane در شبکه، در دستگاهی به نام SDN Controller انجام می شوند.

- ✓ یکی از اولین کارهایی SDN Controller، پس از اتصال به شبکه انجام می دهد، کشف و درک Network Topology است.
- ✓ SDN Controller زیرساخت شبکه را فرماندهی می کند.

- ✓ هر Network Device ای که به شبکه اضافه یا از شبکه حذف شود، SDN Cntrllr فوری متوجه می شود.
- ✓ هر Network Device ای که به شبکه اضافه می شود، در صورت موردتایید بودن، بطورخودکار همه ی پیکربندی های اولیه را از SDN Cntrllr دریافت می کند، که به این قابلیت، Zero-touch provisioning گفته می شود.

بطورکلی دوحالت برای راه اندازی SDN وجود دارد:

Imperative یا دستوری و امری:

- ✓ بطورمثال Routing Protocol ای (OSPF, EIGRP) بر روی Network Device ها اعمال و اجرا نمی شود، اما خود Router ها، همچنان Routing Table شان را دارند که مسیرهای موردنظر بر روی آنها تعریف شده و بسته ها را بر اساس آن انتقال می دهند، اما این جدول های مسیریابی را SDN Controller به سوی آنها ارسال و بر روی آنها تعریف و ایجاد می کند، و هر لحظه امکان تغییر و بروزرسانی این جدول ها، از سوی خود SDN Controller وجود دارد.
- ✓ در این مدل، در صورت بروز هرگونه اختلال برای SDN Cntrllr، کارکرد شبکه، مختل خواهد شد.

Declarative یا اعلامی:

- ✓ در این حالت، Control Plane اصلی درون خود SDN Controller است، اما Control Plane هریک از Network Device ها بر روی آنها فعال و آماده بکار هستند.
- ✓ می دانیم که نیازهای اصلی Client ها تشکیل شده است از کار با نرم افزارها و نه هیچ چیز دیگر
- ✓ Client ها از Software های متفاوتی استفاده می کنند.
- ✓ هریک از این Software ها مثل همه ی ارتباط های معمولی شبکه، اطلاعات خود را به شکل Packet، در شبکه جابجا می کنند.
  - ○ در گذشته، بدون توجه به اینکه Packet های هر Software، به چه مقدار از منابع سخت افزاری شبکه نیاز دارند، Packet ها در شبکه ارسال و دریافت می شدند، مگر اینکه به شکل Policy های مختلف بر روی Network device ها، این نیازمندی ها را برای هر ترافیک خاص، تعریف می کردیم. این منابع شامل موارد متفاوتی هستند، مثل: مقدار Bandwidth ، میزان Speed ، وزن prority ، میزان delay قابل تحمل و ... .

- ✓ اما در مدل Declarative شبکه های SDN، به محض آغاز ارسال بسته های یک Software در شبکه، دستگاه SDN Controller، آگاه می شود و شرایط و policy های مورد نیاز آن نرم افزار را مشخص کرده و به همه ی Network Device های شبکه ارسال می کند که همه ی اعضای شبکه از وجود این نرم افزار مطلع شده و Policy هایی که SDN Controller تعیین کرده را، برای او اجرا کنند.
- ✓ اما جزییات مسیریابی دقیق و محاسبات دقیق تر Packet ها در شبکه، بر عهده ی خود Control Plane های روی Network device ها خواهد بود.
- ✓ پس SDN Controller، نرم افزارها فعال و وارد شده را شناسایی و محدودیت ها و نیازها و اولویت آنها را مشخص و به Network device ها همه ی شرایط را اعلام می کند. به این معنی که، اینکه چطور بسته ها تحلیل و مسیریابی و ارسال می شوند، ربطی به SDN Controller ندارد، اما شرایطی که SDN Controller گفته است، باید لحاظ شوند.
- ✓ پس بر روی Network Device ها، هم Routing Protocol ها فعال هستند و هم پروتکل های QoS و ... .
- ✓ در این مدل، در صورت بروز هرگونه اختلال برای SDN Cntrllr، کارکرد شبکه، مختل نخواهد شد.

Nano Server :

Nano Server یک نسخه ی محدود شده و کم حجم از Windows Server است که به طور خاص برای اجرای برنامه های کاربردیِ تحت Cloud و بی نیاز به تجهیزات و سخت افزارهای فوق العاده سنگین، ایجاد و با نام Tuva معرفی شده است.

رابط کاربری گرافیکی (GUI) و همچنین ویژگی های دیگر در Nano Server حذف شده اند؛ که به همین جهت، این ویندوز می تواند سرعت، پایداری و امنیت بیشتری را برای کاربران ارائه داده و مصرف استفاده از سخت افزار را به طور چشمگیری کاهش دهد.

درصد خطای Nano Server بسیار پایین است و مشکل Reboot شدن را نسبت به Windows Server، تا بیش از 80 درصد کاهش داده است.

در Nano Server هیچ گونه ورود به Remote Desktop وجود ندارد و برای مدیریت سرور، تنها باید از طریق CMD WMI و PowerShell اقدام کرد.

- NanoServer فقط با ابزارها و نرم افزارهای 64 بیتی کار می کند.
- تنها به صورت مجازی و تحت HyperV قابل راه اندازی است.
- Nano Server در اصل یک سیستم Headless است، یعنی امکان Local Login در این نسخه از سرور وجود ندارد.
- نمی توانیم روی آن Active Directory داشته باشیم.
- Group policy را پشتیبانی نمی کند.
- می توان دستورهای PowerShell DSC را در آن اجرا کرد؛ اما فقط از نوع Push.
- قابلیت تنظیم Proxy برای ارتباط با اینترنت را ندارد.
- Nano Server نیازی به فعال کردن (Activate) ندارد.
- بیشتر به منظور راه اندازی Hyper-V و DataCenter طراحی و عرضه شده است.
- تمام تنظیمات به صورت Remote انجام می‌شوند، چون این سرور برای اجرا و مدیریت سرویس ها از راه دور طراحی شده است.
- سرورهای نانو، توانایی اجرا کردن برنامه های با محیط گرافیکی را ندارند.
- Nano Server برای محیط زیرساخت ایجاد شده است.

برخی خصوصیت های Nano Server :

- تعداد پورت‌های بازِ کمتر
- سرویس‌های مورد نیاز کمتر در هنگام کارِ Server
- Driver های سخت افزاری کمتر
- نیازِ خیلی کم به منابع
- امنیت بهتر نسبت به نسخه‌ی Core

Nano Server مثل سایر نسخه‌های ویندوز، قابل نصب مستقیم بر روی سخت افزار نیست، بلکه با طی کردن مراحلی، آن را تنها بر روی یک VHD توسعه داده و در نهایت آن VHD را در یک Hyper-V می‌توان استفاده کرد.

: PowerShell Nano Server-Implementation

درست مثل نسخه های Desktop و Core، می توانیم نسخه ی Windows Nano را نیز هم بر روی VM ها و هم بر روی سیستم فیزیکی نصب کنیم.
یعنی می توانیم Nano Server را به عنوان یک سیستم Host راه اندازی کرده و بر روی آن، VM هم ایجاد کنیم، که زیاد انجام نمی شود!

تنظیمات اولیه را انجام می دهیم:

- ابتدا DVD مربوط به Windows Server 2016 و یا Image آن را وارد می کنیم.
- باید دستورات مرتبط با Nano Server وارد کنیم. وارد PowerShell شده و درج می کنیم (X نام درایو DVD یا Image است):

```
Import-Module X:\NanoServer\NanoServerImageGenerator -Verbose
```

در طی این راه اندازی NANO Server، پس از هربار Restart، احتمالاً لازم است که این دستور Import انجام شود.

1. Nano Server را ایجاد می کنیم.

- توسط دستور زیر، فایلِ سیستم عامل Nano Server ای که دارای سرویس IIS است را ایجاد می کنیم:

```
New-NanoServerImage -MediaPath D:\ -BasePath C:\Folder1\Base-Path `
-TargetPath C:\Folder1\NanoHD.vhdx -DeploymentType Guest -Edition Datacenter -ComputerName NPC `
-InterfaceNameOrIndex Ethernet -Ipv4Address 192.168.139.150 -Ipv4SubnetMask 255.255.255.0 -Ipv4Gateway 192.168.139.1 `
-Ipv4Dns("192.168.139.139","8.8.8.8") -Package Microsoft-NanoServer-IIS-Package `
-AdministratorPassword (ConvertTo-SecureString -AsPlainText "xxxx" -force)
```

- **Mediapath** : نام درایو DVD یا Image ویندوز Server است.
- **BasePath** : مسیر ذخیره ی تنظیمات این Nano Server در سیستم می باشد.
- **TargetPath** : مسیر ایجاد یک حافظه ی مجازی برای آن می باشد که باید فرمت vhdx داشته باشد.
- **DeploymentType** : اگر بخواهیم این NANO Server
  - بعنوان VM کار کند: Guest
  - بعنوان Host کار کند: Host
- **Edition** : دو نوع نسخه ی Standard و Datacenter را پشتیبانی می کند.
- **ComputerName** : یک نام دلخواه برای سیستمی که ایجاد می شود.
- یک NIC برای آن ایجاد کردیم به نام : Ethernet
- آدرس های IP و DNS و DG را برای آن تعیین کردیم.
- مشخص کردیم که کدام Windows Feature (در NANO Server به نام Package) نصب شود. (مثلاً IIS)
- برای اطلاع یافتن از نام Feature (Package)های دیگر، می توانیم به آدرس C:\Folder1\BasePath\Packages که ایجاد کردیم، برویم.

2. اگر ابزار HyperV نصب نیست، آنرا نصب و یکبار Restart می کنیم:

```
Install-WindowsFeature hyper-v -IncludeAllSubFeature -IncludeManagementTools
```

3. یک Virtual Machine ایجاد کرده و Nano Server را به آن متصل می کنیم.

- ابتدا توسط دستور زیر، نام کارت شبکه های سیستم را پیدا می کنیم:

```
Get-NetAdapter
```

- وارد کنسول HyperV شده و در ابزار Virtual Switch Manager، یک External Switch ایجاد می کنیم به نام ExSwitch.
  و یا در PowerShell توسط دستور زیر، یک VSwtich ایجاد می کنیم:

```
New-VMSwitch -name ExSwitch -NetAdapterName Ethernet0 -AllowManagementOS $true
```

- سپس در PowerShell دستور زیر را وارد می کنیم:

```
New-VM -Name VNS -VHDPath C:\Folder1\NanoHD.vhdx -MemoryStartupBytes 1GB -SwitchName ExSwitch -Generation 2 |
Start-VM
```

- وارد کنسول HyperV شده و به VM ایجاد شده، Connect می کنیم.
- برای User درج می کنیم: Administrator و برای Password : پسوردی که تعریف کرده بودیم را درج کرده و اینتر.
- تمامی دکمه های کنترلی را در پایین صفحه می بینیم.
- از تنظیمات IP مطمئن می شویم.
- از آنجایی که تنظیمات این Server معمولاً از راه دور و توسط Windows Remote management (WinRM) است، و با ایجاد کوچکترین تغییرات در تنظیمات آن ارتباط خدشه دار می شود، می توان وارد گزینه ی WinRM شده و با Enter و تأیید مجدد، آنرا به حالت اولیه که فعال نیز می باشد، بازگرداند.

نکته: WinRM با دو پورت **5985 HTTP** و **5986 HTTPS** کار می کند.

4. NANO Server را کنترل می کنیم.

- همانطور که می بینیم، تنظیمات خاصی را نمی توانیم روی NANO Server اعمال کنیم.
- پس از سیستم Host و توسط PowerShell از قابلیت PowerShell direct استفاده می کنیم.
- پس در PowerShell دستور زیر را درج کرده و با Admin User مربوط به NANO Server وارد و با دستور زیرین، خارج می شویم:

```
Enter-PSSession -VMName VNS
Exit-PSSession
```

- می توانیم توسط دستور زیر فعال بودن IIS را بررسی کنیم:

```
Get-Service w3svc
```

- وقتی IIS نصب می شود، در درایو C پوشه ی inetpub ایجاد می شود، برای اطمینان از آن:

```
Get-ChildItem -Path c:\inetpub
```

- در حقیقت اگر Firewall این NANO Server را برای Public، خاموش کنیم، با درج نام یا آدرس آن و هریک از درایوهای آن در یک Explorer در شبکه، می توانیم وارد آن درایو از این سیستم شویم:

\\\\192.168.139.150\C$

- برای اینکه بتوان به یک NANO Server عملیات Ping را انجام داد، باید وارد Inbound Firewall Rules و سپس In – ICMPv4 – Echo Request شده و آن را Enable کنیم.

- اگر باز هم Ping انجام نشد، توسط دستور زیر Firewall را برای Domain و Public غیرفعال می کنیم:

```
Set-NetFirewallProfile -Name public,domain -Enabled False
```

- اگر زمان و یا تاریخ آن اشتباه است، Time Zone آنرا تصحیح کنید.

نکته: در NANO Server ها، دستور systeminfo که مشخصات سیستم را می دهد، کار نمی کند.

Wizard Nano Server-Implementation :

با فرض اینکه هیچ اطلاعی از نحوه ی راه اندازی NANO Server توسط PowerShell نداریم، و فقط Hyper-V را نصب کرده ایم:

- توسط یک Search در Internet به دنبال Nano Server Image Builder.msi، این نرم افزار کوچک را از سایت Microsoft دانلود کرده و بر روی سیستم Host، نصب می کنیم.
  - پس از نصب آنرا از طریق Start ویندوز، پیدا و Open می کنیم که احتمالاً خطا می دهد که باید دو ابزار Deployment Tools و Windows PE را نصب کنیم.
  - پس اگر درخواست دانلود آن فایل را داد، Ok کرده و دانلود می کنیم و یا اینکه توسط یک Search در Internet تحت عبارت download windows assessment and deployment kit، فایلی که لینک آن به نام Download the Windows ADK for Windows 10، در سایت Microsoft وجود دارد را دانلود کرده و وارد مراحل نصب آن می شویم.
- گزینه ی ...Download the Windows Assessment and Deployment Kit را زده و یک آدرس برای آن مشخص می کنیم. مثلاً : C:\ADK
- برای ..Send Anonymous u ، گزینه ی No را زده و تا پایان دانلود پیش می رویم.
- پس از دانلود، وارد محل دانلود آن شده و فایل exe. را باز کرده و اینبار گزینه ی ..Install the Windows Assessment را انتخاب و پیش می رویم.
- تمام گزینه های تب Select Features را (به جز مثلاً Microsoft SQL Server) انتخاب و نصب می کنیم.
- Nano Server را ایجاد می کنیم.
- پس از نصب، وقتی وارد Start ویندوز شویم، ابزارهای آن، به گزینه های بالا سمت چپ اضافه شده اند، برای مشاهده ی همه، Expand را زده و سپس وارد Nano Server Image Builder می شویم.
- همانطور که دیده می شود، دو قابلیت وجود دارد:
  - ایجاد یک Nano Server Image که می توان آن را از طریق Virtual Machine ها اجرا کرد.
  - ایجاد یک USB Bootable NANO Server
- گزینه ی اول را زده و در تبی که باید Windows Server Media Source انتخاب شود، درایو DVD یا Image ویندوز سرور را انتخاب می کنیم.
- در تب انتخاب Deployment Type، گزینه ی Virtual Machine Image را زده و یک مسیر و یک نام با فرمت vhdx. برای ذخیره ی آن تعیین می کنیم و در پایین همین تب، مقدار حافظه ی آن را تعیین می کنیم که باید از 8 GB بیشتر باشد.
- در تب Optional Packages هم نسخه ی ویندوز را و هم هریک از Package های موردنظر را انتخاب کرده و Next.
- اگر NANO Server قرار بر نصب بر روی یک سیستم سخت افزاری است، یا حتی بصورت USB Bootable، که این سخت افزار، نیاز به یک سری Driver ها دارد، آنها را در تب Add Drivers انتخاب می کنیم.
- یک Name و رمز عبور در تب Destination Machine تعریف می کنیم.
- در تب Join Domain اگر گزینه ی Domain Name را بزنیم و آدرس Root Domain را وارد کنیم، باید قبل از آن، در AD شبکه، یک Computer دقیقا با نامی که در تب قبل وارد کردیم، برای آن ایجاد کرده باشیم. اما در اینجا آن را غیرفعال کرده و Next.
- گزینه ی Enable WinRM را فعال کرده و بقیه ی تنظیمات را رها می کنیم و Next.
- می توانیم آن را در همینجا بصورت یک Image با تنظیمات پایه ای ایجاد کنیم، و یا با انتخاب گزینه ی Advanced Setting تنظیمات دیگری را به آن اضافه کنیم، که سپس باید تنظیماتی را نیز در چند تب جدید، انجام داد و تا Create پیش رفت.
- پس از اتمام، فایل آن در مسیر تعیین شده، ایجاد می شود که قابلیت Mount شدن نیز خواهد داشت!
- توسط دستور زیر، برای این Nano Server یک VM ایجاد می کنیم:

```
New-VM -Name NANoHD3 -VHDPath C:\Folder1\NANO-3.vhdx -MemoryStartupBytes 1GB -SwitchName ExSwitch -Generation 2 | Start-VM
```

:Join a NANO Server to Domain

نکته: Join کردن یک Nano Server به Domain به صورت Offline انجام می شود!

- قبل از هرچیز، وارد VM و گزینه ی WinRM شده و آن را Confirm می کنیم.
- Nano Server باید توسط یک Virtual Switch به شبکه متصل شده باشد.
- وارد تنظیمات Networking شده و IP آن را مشاهده می کنیم.

IP سیستم Host برابر است با : 192.168.139.139

IP سیستم Nano برابر است با : 192.168.139.150 و Computer Name آن : NPC

1. توسط قابلیت Offline Domain Join، سیستم NANO را در Domain عضو می کنیم.

- سیستم Nano Server را روشن نگه می داریم!
- در Host، با دستور زیر، Nano Server را به لیست Server های قابل اعتماد منتقل می کنیم:

```
Set-Item WSMan:\localhost\Client\TrustedHosts "192.168.139.150"
```

- توسط دستور زیر یک Session با Nano Server برقرار می کنیم:

نکته: جهت سرعت عمل در ادامه ی کار، این دستور برقراری ارتباط را، درون یک متغیر قرار می دهیم.

```
$N1 = New-PSSession -ComputerName 192.168.139.150 -Credential(Get-Credential)
```

- برای ODJ کردن Nano Server، توسط دستور زیر، یک Object برای آن در AD و یک فایل blob. ایجاد می کنیم:

```
djoin /provision /domain payamavar.local /machine NPC /savefile C:\Folder1\NANO.blob
```

- به صورت زیر، فایل ایجاد شده را در Nano Server اجرا می کنیم:

```
Copy-Item -Path C:\Folder1\NANO.blob -Destination c:\ -ToSession $N1
```

- می توانیم وارد یک File Explorer شده و درج می کنیم:

\\\\192.168.139.150\c$

- برای دسترسی به فایل کپی شده در NANO Server ابتدا باید FireWall آن را برای Public خاموش کنیم:

```
Enter-PSSession -Session $N1
```

- حال توسط دستور Ipconfig /all مشخصات کامل آن را بررسی کرده و در پایان، با دستور زیر، فایل ایجاد شده را Load می کنیم:

```
djoin /requestodj /loadfile C:\NANO.blob /windowspath C:\Windows /localos
```

- پس از موفقیت آمیز بودن دستور، NANO Server را توسط Restart-Computer یکبار Restart می کنیم.

2. تنظیمات NANO Server را در DC کنترل می دهیم.

- سپس دوباره به سیستم NANO جلسه زده و نحوه ی دریافت IP را بر روی DHCP قرار می دهیم:

```
Enter-PSSession -ComputerName npc
Set-NetIPInterface -InterfaceAlias 'Ethernet0' -Dhcp Enabled
```

- حال اگر به DNS Manager برویم، می بینیم که A Record آن نیز ایجاد شده است.
- جهت کنترل سیستم NANO، می توان در Server Manager از طریق Manage وارد Add Servers شده و گزینه ی آن را نیز اضافه کرد.

3. Package های موردنیاز را نصب می کنیم.

- همانطور که می دانیم، شیوه ی نصب Role ها بر روی NANO Server شباهتی به سیستم های معمولی ندارد، چون بیشتر توسط نصب Package ها، سرویس دهی ها را انجام می دهیم.
- برای دسترسی به Package ها، از ابزارهایی به نام Package Provider استفاده می شود.
- برای مشاهده ی Package Provider های موجود در سیستم، می توان از دستور زیر استفاده کرد:

```
Get-PackageProvider
```

Package Installation :

- برای NANO Server ها، به Package Provider خاص خودشان، به نام Nano Server Package نیاز خواهیم داشت.

نکته: این کار را توسط Administrator انجام می دهیم.

- ابتدا یکبار وارد DNS شده و یکبار وارد Server Manager شده و اضافه شدن NANO Server را چک می کنیم.

نکته: باید هم سیستم Host و هم سیستم NANO، به اینترنت دسترسی داشته باشند، حتی اگر لازم شود، می توان یک Virtual Switch دیگر هم ایجاد و آن را به Internet متصل کرد و یک NIC دوم برای NANO Server ایجاد و به Switch متصلِ به اینترنت، وصل کرد.

ابتدا نام کارت شبکه ی Host که به اینترنت دسترسی دارد را پیدا می کنیم، سپس یک سوییچ مجازی متصل به آن ایجاد می کنیم:

```
Get-NetAdapter
New-VMSwitch -name ExSwitch2 -NetAdapterName Ethernet1 -AllowManagementOS $true
```

حال یک NIC جدید برای VM ایجاد کرده و سوییچ جدید را به آن متصل می کنیم:

```
ExSwitch2
Connect-VMNetworkAdapter -VMName VNS -Name 4Net -SwitchName ExSwitch2
```

- پس به NANO Server (مثل یک عضو شبکه) یک جلسه زده و Internet را تست می کنیم:

```
ping google.com
```

- اگر مشکل داشت، می توان توسط دستورهای /release و /renew یا دستور زیر، کارت شبکه را قطع و وصل کرد:

```
Restart-NetAdapter -Name "Ethernet"
```

- پس از ارتباط با Internet، دستور زیر را وارد می کنیم:

```
Install-Module -Name NanoServerPackage -SkipPublisherCheck -Force
```

برای مشاهده ی آن:

```
Get-InstalledModule
```

- حال آن را نصب می کنیم:

```
Install-PackageProvider Nanoserverpackage
```

- ExecutionPolicy را تنظیم می کنیم:

```
Set-ExecutionPolicy RemoteSigned -Scope Process
```

- Package نصب شده را درون Nano Server وارد می کنیم:

```
Import-PackageProvider NanoServerPackage
```

- برای مشاهده ی تمامی Package های موجود، از دستور زیر و برای مشاهده ی Package های مربوط به NANO Server از یکی از دستورهای زیرین استفاده می کنیم:

```
Find-Package

Find-Package -ProviderName NanoServerPackage
Find-NanoServerPackage | select name
```

- حال برای نصب هریک از Package های بالا، به صورت زیر عمل می کنیم (مثلاً برای نصب DNS):

```
Install-NanoServerPackage -Name Microsoft-NanoServer-DNS-Package
```

از Session خارج می شویم.

توسط دستور زیر می توانیم ببینیم که همچنان سیستم NANO جزو سیستم های اعتماد شده است:

```
get-Item WSMan:\localhost\Client\TrustedHosts
```

برای حفظ امنیت، این اعتماد سازی را توسط دستور زیر، از بین می بریم:

```
Set-Item WSMan:\localhost\Client\TrustedHosts ""
```

Windows Migration :

فرض کنید که یک DNS Server یا DHCP Server داریم که دارای ویندوز سرور 2012 می باشد، و می خواهیم بدون مشکل و خسارت، این ویندوز را به Server 2016 تبدیل کنیم.

می توان از روش Windows Upgrade استفاده کرد، اما روش مطمئن تر، Migration است.

ابتدا یک Windows Server 2016 بر روی یک سیستم دیگر کاملاً معمولی و صحیح نصب می کنیم، که به آن Clean Install هم گفته می شود. و این سیستم هنوز به هیچ شبکه ای متصل نیست.

فرض کنید بر روی یک Server که دارای ویندوز نسخه ی Server 2012 می باشد، DHCP Server شبکه قرار دارد.

1. تنظیمات Destination Server را انجام می دهیم.

- وارد PowerShell مربوط به Server 2016 شده و برای بررسی وجود Feature مربوط به Migration درج می کنیم:

```
Get-WindowsFeature migration
```

- اگر نبود:

یا به Add Roles and Features رفته و در قسمت انتخاب Feature ها، Windows Server Migration Tools را انتخاب و نصب می کنیم؛ و یا با دستور زیر در PowerShell:

```
Install-WindowsFeature -Name migration
```

- دستور زیر را وارد می کنیم، تا به این Directory برویم یا به اصطلاح، navigate شود:

```
cd C:\Windows\System32\ServerMigrationTools
```

- دستور زیر را وارد می کنیم، تا بسته ای برای سیستم مبدأ (با توجه به نسخه ی ویندوز مبدأ) ایجاد شود(Server 2012R2):

```
.\SmigDeploy.exe /package /architecture [amd64 |x86] /os [WS16|WS12R2|WS12|WS08|WS08R2|WS03] /Path [Directory]

.\SmigDeploy.exe /package /architecture WS12R2 /Path C:\Folder1
```

در حقیقت در آدرسی که در این دستور درج کردیم، یک Package ایجاد می شود به نام SMT_ws12R2_amd64، که مثل یک ظرف است که باید به سیستم مبدأ (Server 2012) انتقال دهیم تا محتویاتش را درون این ظرف بریزد. پس فایل ایجاد شده را به Server 2012 برده و مثلاً در آدرس C:\Folder2\ قرار می دهیم.

2. عملیات Migration را در Source Server انجام می دهیم.

- باید نرم افزار Netframework 3.5 را نصب باشد، پس توسط دستور زیر چک می کنیم:

```
Get-WindowsFeature net-framework-core
```

- اگر نبود، DVD (Image) ویندوز سرور 2012 R2 را وارد می کنیم و دستور زیر را در PowerShell درج می کنیم:

```
Install-WindowsFeature net-framework-core -Source X:\sources\sxs
```

- بسته ی SMT_ws12R2_amd64 را اجرا می کنیم:

```
C:\folder2\SMT_ws12R2_amd64\smigdeploy.exe
```

صفحه ی PowerShell باز شده را می بندیم.

- اگر دستور زیر را بزنیم، می بینیم که هیچ دستوری جهت عملیات مهاجرت وجود ندارد:

```
Get-Command -Module *Migration*
```

باید این دستورات را اضافه کنیم، پس دستور زیر را وارد کرده و دوباره دستور بالا را تست می کنیم:

```
Add-PSSnapin Microsoft.Windows.ServerManager.Migration
```

- توسط دستور زیر، می توانیم ببینیم که کدام Feature ها، قابلیت مهاجرت کردن را دارند:

```
Get-SmigServerFeature
```

نکته: برای migrate کردن هریک از Feature های موردنظر، باید ابتدا آن را inactive کنیم.

- پس درج می کنیم:

```
Stop-Service -Name DHCPServer
```

- توسط دستور Get-Command در بالا، ID مربوط به DHCP را پیدا می کنیم و توسط دستور زیر آن را Export می کنیم:

```
Export-SmigServerSetting -FeatureId DHCP -Path c:\folder2\mig -Verbose
```

جهت حفظ امنیت، یک **Password** برای آن تعیین کردیم، و سپس در پوشه ای دلخواه (**mig**) ذخیره می شود.

- حال فایل ایجاد شده را به **Server 2016** برده و مثلاً در آدرس **\C:\Folder1** قرار می دهیم.

3. عملیات Migration را در Destination Server را انجام می دهیم.

- دستورات مربوط به **Migration** را نصب می کنیم:

```
Add-PSSnapin Microsoft.Windows.ServerManager.Migration
```

- حال فایل **Migration** را **Import** و نصب می کنیم:

```
Import-SmigServerSetting -FeatureId dhcp -Path c:\Folder1 -Verbose -Force
```

- حال در کنسول **Server Manager** می بینیم که **DHCP Server** اضافه شده است، پس آنرا **Commit** می کنیم.
- اما کنسول **DHCP Manager** نصب نیست، پس وارد **Add Roles and Features** شده و بدون تغییر پیش می رویم، اما در بخش **Feature**، از زیرگزینه های **Remote Server Administration Tools**، گزینه ی **Role Administration Tools** و سپس گزینه ی **DHCP Server Tools** را انتخاب کرده و نصب را تا پایان پیش می رویم.
- وارد کنسول **DHCP** شده و تنظیمات را بررسی می کنیم، اگر **Error** داده و با موفقیت باز نشد، دوباره وارد **PowerShell** شده و یکبار دیگر عملیات **Import** را انجام می دهیم.

Network designing :

:Required Servers and Accessories

❖ هر شرکت یا سازمانی با اندازه ی متوسط، حداقل به تعدادی Server نیازمند است:

1. First Server : Firewall

معمولا اولین Server شرکت‌ها، مثل درگاهی ست که میان شبکه و اینترنت قرار دارد و سیستم Firewall روی آن قرار دارد.
با ورود اینترنت پر سرعت به شرکت ها، نیاز به کنترل آن احساس می‌شود.
بهینه‌سازیِ استفاده از اینترنت و حفظ ورود و خروج اطلاعات، برای هر شرکتی مهم است و به اندازه ی شرکت و تعداد کارمندان آن ارتباطی ندارد.
بهتر است ورود و خروج اطلاعات بر عهده ی یک Server باشد که توسط نرم افزارهای امنیتی مدیریت می‌شود.
این نرم افزارها توانایی کنترل ورود و خروج کاربران و اطلاعات را به عهده می‌گیرند. این نرم افزارها بررسی می کنند که اطلاعاتی که وارد سیستم کاربران می‌شوند، خالی از آلودگی‌های امنیتی باشند.
به غلط در شرکت‌های کوچک مرسوم شده که اشتراک‌گذاری اینترنت را بر عهده ی Switch قرار می‌دهند و هیچ سیاست ورود و خروج اطلاعاتی در نظر گرفته نمی‌شود، یعنی مودم ADSL به عنوان Router و ورودی اینترنت، بطور مستقیم به Switch وصل می‌شود و همه ی کاربرها بدون هیچ گونه کنترل و مدیریت، از اینترنت استفاده می‌کنند، از این رو چون هیچ سیستم کنترلی و مدیریتی برای حفظ امنیت کاربرها وجود ندارد، به سادگی دچار خسارت های امنیتی می‌شوند.
توصیه می شود که کنترل ورود و خروج اطلاعات با روش های کاملاً ایمن و اصولی انجام شود و اینترنت بصورت مستقیم روی شبکه Share نشود و از برنامه‌هایی مثل WinRoute Kerio Control یا ISA Server، امنیت لازم برای شرکت فراهم شود.

2. Second Server : Active Directory

معمولا Active Directory و سرویس‌های آن، راه اندازی شبکه ی Local سازمان را میسر می‌سازند.

3. Third Server : Financial and office software (نرم افزار مالی و اداری)

می دانیم که هر شرکتی با هر اندازه ای، برای ساختار حسابداری خود، مجبور به استفاده از حداقل یک نرم افزار حسابداری و انبارداری است.
معمولا این برنامه ها دارای قفل سخت افزاری نیز هستند، پس برای دور نگه داشتن و حفاظت از این قفل سخت افزاری از دسترس عموم، باید آن را بر روی یک Server مجزا راه اندازی کرد.
معمولا دسترسیِ فیزیکی به چنین Server هایی، محدودتر از دیگر Server هاست.
درحقیقت نرم افزاری که توانایی ذخیره سازی اطلاعات مالی را دارد، نیاز به یک Database هم دارد تا بتواند اطلاعات بازه های زمانی طولانی را نیز در خود ذخیره کند.
می‌توان بانک های اطلاعاتی SQL یا MYSQL را به راحتی یا در همین Server و یا Server شماره 2 راه اندازی کرد.

❖ تا اینجا که ضرورت وجود حداقل سه Server را می دانیم، نیاز به یک محل مناسب برای قرارگیری آنها داریم.
پس از یک Rack ایستاده (Standing Rack) استفاده می کنیم که با تهویه ی مناسب، حرارت تولید شده از این Server ها را از داخل Rack، خارج و هوای خنک را وارد کند.

4. Fourth Server : File Server / Storage Server

گرفتن Backup از اطلاعات موجود، یکی از امور ضروری در شبکه است؛ آن هم به صورت روزانه.
اضافه کردن یک هارد دیسک داخلی کار زیاد سختی نیست، اما زیاد هم عقلانی نیست.
معمولاً Backup را بر روی یک دستگاه خارجی می‌گیریم تا در زمانی که Server، مورد حمله ی ویروس ها یا Hacker ها قرار گرفت و یا دیسک آن دچار خرابی شد و غیرقابل بازیابی شد، خارج از Server، یک نسخه از تمام اطلاعات داشته باشیم.
به دستگاهی سریع و مطمئن نیاز داریم که به راحتی عملیات Backup از Server ها و حتی Client ها را انجام دهد.
به همین جهت، از یکی از دستگاه های NAS Server یا SAN Server استفاده می شود، که هریک، خود دارای سیستم عامل می باشند.

5. Fifth Server : CRM Server

در بسیاری از شرکت ها، رضایت مشتری، حفظ مشتری و مدیریت مشتری و حتی طبقه‌بندی مشتری ها، اهمیت زیادی دارد و نیاز به سیستم‌های اتوماسیون اداری، سیستم‌های مدیریت اطلاعات مشتری ها، **Web Server**، **Mail Server** و ... چیزیست که از آن نمی‌توان چشم‌پوشی کرد.
پس به یک **Server** برای راه اندازی این ابزار نیاز خواهیم داشت.

- برای کاهش نگرانی‌های روزانه از امنیت روشن و بکار بودن **Server** ها، به یک سیستم نگهدارنده ی انرژی برق هم نیاز داریم تا در صورت قطعی برق، حداقل چند **Server** را همیشه روشن نگه دارد و سرویسدهی متوقف نشود.

- برای حفظ امنیت **Server** ها و دور از دسترس بودن آنها، محل نگهداری آنها باید در محیطی بسته و مهر و موم شده و درون **Rack** باشد.
- بهترین پیشنهاد برای محل نگهداری **Rack** و **Server** ها، راه اندازی یک اتاق **Server** است.

DHCP :

در حقیقت در شبکه های **Workgroup** آدرس **IP** هریک از **Client** ها باید به صورت **Static** و در یک **Range** تنظیم شود.
در بسیاری از موارد، یک **DHCP Server** آنقدر سنگین نیست، پس به جای آن‌که آن را در یک سرور اختصاصی نصب کنید، می‌توان در **Server** های موجود مثل **Domain Controller**، سرویس **DHCP Server** را نیز نصب کنید.
به هرحال، در صورت راه اندازی یک سیستم جدا برای **DHCP**، باید دقت کرد که علاوه بر کامپیوتر **Domain Controller**، کامپیوتر **DHCP Server** نیز حتماً باید یک آدرس **Static** داشته باشد.

یکی از وظایف **Active Directory**، جلوگیری از قرارگیری **DHCP Server** های مخفی یا غیرمجاز و هماهنگ نشده در شبکه است.
به این صورت که ما نمی خواهیم **Server** های تأیید نشده که به اختصاص **IP** به کامپیوترهای شبکه مان می‌پردازند را داشته باشیم.
علاوه بر **Microsoft** سیستم های دیگری هم می توانند در شبکه وجود داشته باشند که دارای سرویس **DHCP** باشند، مثل **Linux** و ...
و کنترل یا جلوگیری از این **DHCP** ها، کار را برای سیستم های **Microsoft** سخت تر می کند.

معمول‌ترین سرورهای **DHCP** غیرمجاز، **Router** ها یا **Access Point** هایی هستند که به همراه **DHCP** پیشفرض(**Built-in**) عرضه می‌شوند.
داشتن چندین سرور **DHCP** در یک شبکه، کاملاً منطقی است، زیرا درجه‌ای از تحمل خطا را در شبکه فراهم می‌کند.
به هر حال باید از اختصاص دادن **IP** مناسب که با **DHCP** دیگر تداخل نداشته باشد، اطمینان پیدا کنید.

برای اطمینان از نبود یک **DHCP Server** دیگر در شبکه، می توان یک **Client** را برای دریافت خودکار **IP** تنظیم کرده و آن را دوباره راه‌اندازی نمود.
اگر آدرس **IP** دریافت کرد، یعنی یک **DHCP Server** غیرمجاز یا هماهنگ نشده در شبکه وجود دارد، در غیراین‌صورت، حله!

Speed :

در حقیقت یکی از پیشنیازهای اولیه در طراحی و اتصال شبکه ها به یکدیگر، دانایی از میزان سرعت هریک از **Site** ها می باشد.
باید در **Active Directory** مشخص کنید که:

- در شبکه ی ما چه تعداد **Site** وجود دارد و هریک با چه سرعتی کار می کنند.
- **Replication** بین **Site** ها با چه سرعتی و هرچند وقت انجام شود.
- هرقدر که سرعت بین دو **Site** بیشتر باشد، می توان تعداد دفعات **Replicate** آنها در روز را بیشتر کرد.
- به عبارت دیگر، هرقدر نیاز به تعداد دفعات بیشتری **replication** در یک فاصله ی زمانی کوتاه تر باشد، باید برای افزایش سرعت بین شبکه ای، هزینه کرد و تجهیزات مناسب را تهیه کرد.

امروزه حداقل سرعت مناسب در شبکه های **local** برابر با **1 Gbit/Sec** است.
تعداد **Domain** های یک شبکه هیچ ربطی به تعداد **Site** های آن ندارد.
می توان 5 سایت را تحت یک **Domain** ، شبکه کرد و یا آنها را با **5 Domain** ، شبکه کرد.

Troubleshooting the Network:

User Account status

تنها با داشتن بخشی از یک **Username**، توسط دستور زیر می توان اطلاعاتی شامل زمان ایجاد، آخرین **login**، فعال یا غیرفعال بودن آن **Account** را بدست بیاوریم:

```
Get-ADUser -Filter 'Name -like "*xxx*"' -Properties "LastLogonDate","whenCreated", "SamAccountName", "distinguishedname" | select name, SamAccountName, whenCreated, LastLogonDate, enabled, distinguishedname | Format-List
```

The real last login time

درحقیقت در شبکه های پیچیده و بزرگ، توسط دستور بالا، به سادگی نمی توان آخرین ورود دقیق یک **Account** را در شبکه، بدست آورد، بلکه یک زمان نادقیق یا حتی خیلی قدیمی تر را نشان خواهد داد، پس توسط دستور زیر، آخرین زمان بازدید دقیق را بدست خواهیم آورد:

```
$username = "xxx"
[datetime]::FromFileTime((Get-ADDomainController -Filter * | foreach {Get-ADUser $username
-Properties LastLogon -Server $_.Name | select LastLogon} | Measure-Object -Property LastLogon
-Maximum).Maximum)
```

Assign an Account to another Person

فرض کنید قصد داشته باشیم یک **Account** را از اختیار یک شخص خارج و در اختیار شخصی دیگر قرار دهیم.

1. ابتدا آن را **Disable** می کنیم.
2. نام آن را تغییر می دهیم.
3. پسورد آن را تغییر می دهیم.

پس در **PowerShell**:

Disable-ADAccount -Identity نام اکانت

Get-ADUser -Identity نام1 اکانت | Rename-ADObject -NewName نام2 اکانت

در حقیقت، ما تا اینجا، نامی را که این **User** با آن، در محیط **Server** نمایش داده می شود را تغییر داده ایم و نه **UPN** که برای **login** و ... بکار می رود!

پس:

Set-ADUser -Identity نام1 اکانت -SamAccountName نام2 اکانت -UserPrincipalName نام2 اکانت@payamavar.local -DisplayName نام2 اکانت -GivenName نام2 اکانت

Set-ADAccountPassword -Identity نام2 اکانت -Reset

و در پاسخ، یک پسورد مناسب را وارد کرده و در پایان آن را **Enable** می کنیم.

Enable-ADAccount -Identity نام2 اکانت

Assigning IP with DHCP doesn't Work in VMware

اول باید همه ی **VM** ها رو خاموش کنیم، بعد در پنجره ی **Virtual Network Editor** ، در پایین سمت چپ، دکمه ی **Restore Defaults** رو می زنیم.در پایان، تیک **.. Use local DHCP Service to** را برداشته و **OK**!

سپس در تنظیمات کارت شبکه ی تک تک **VM** ها، فقط گزینه ی **Host-Only** را انتخاب می کنیم.

در هریک از **VM** ها، نحوه ی دریافت **IP** را از طریق **DHCP** قرار می دهیم.

Error 1722

اگر هنگام **Replication** فایل های **NTDS** (مثلاً در کنسول AD Sites and Services) با **Error : 1722** ، مبنی بر

The RPC Server is unavailable

مواجه شدیم، به این معنی است که این **Server** قادر به **Replication** با **Active Directory** نیست، که به یکی از دلایل زیر است:

- **Domain controller is in offline state (or broken).**
- **Changes have been made to the network or new firewall rules have been added.**
- **Incorrect DNS configuration on domain controllers or invalid DNS records.**
- **Poor network performance or large delays.**

Error 41

وقتی سیستم **Server**، فوری خاموش یا **Shut Down** می شود، این **Error** در پنجره ی **Server Manager** نمایش داده می شود.

Kerberos Target Resolution Error

اگر در کنسول **Server Manager** و در بخش **All Servers** برای یکی از سیستم ها، این **Error** مشاهده شد، به احتمال خیلی زیاد، دلیل آن مشکلات **Forward Lookup** و **Reverse Lookup** است که باید آنها را بررسی و منظم کرد و اگر نیاز به اضافه کرن یا حذف یک رکورد بود، آن را انجام دهیم.

Not Ping to a Client

اگر در شبکه، ارتباطات با یک سیستم برقرار است، اما وقتی به آن **Ping** می کنیم، با شکست مواجه می شود.

- یا باید **Windows Firewall** را در قسمت **Domain network** غیرفعال کنیم.
- یا باید در آن سیستم، وارد **cmd** شده و:
  - برای **IPv4** دستور زیر را وارد کنیم:

netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow

  - برای **IPv6** دستور زیر را وارد کنیم:

netsh advfirewall firewall add rule name="ICMP Allow incoming V6 echo request" protocol=icmpv6:8,any dir=in action=allow

برای غیرفعال سازی دستورات بالا:

- برای **IPv4** :

netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=block

- برای **IPv6** :

netsh advfirewall firewall add rule name="ICMP Allow incoming V6 echo request" protocol=icmpv6:8,any dir=in action=block

No Connection to other Servers

وقتی یک **Server** به **Server** های دیگر متصل نمی شود، مشکل در **DNS Server** است.

احتمالاً **Name** یا **IP** آن به درستی ثبت نشده است.

Unable to download from URI 'https://go.microsoft.com/

بطور معمول هنگام استفاده از دستوراتی که نیاز به **Internet** دارند مثل **update** ، همچین خطایی می آید، برای رفع آن، دو دستور زیر به ترتیب وارد کرده و **در پایان یکبار Restart** می کنیم:

```
Install-Module PowershellGet -Force

#for 64bit
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord

#for 32bit
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto'  -Value '1' -Type DWord
```

Error: the update is not applicable to your computer

بطورمعمول موقع نصب **RSAT** این **Error** را دریافت می کنیم.

با دسترسی **Admin** وارد **cmd** شده و دستور **sfc /scannow** را وارد می کنیم و صبر می کنیم و تمام!

Boot loader failed - time out

اگر پس از روشن کردن یک **Virtual Machine** در **HyperV** برای نصب ویندوز، با خطای **server the boot loader failed - time out** مواجه شدیم، کافی ست که یکبار **VM** را از نو روشن کرده و یک دکمه ی دلخواه از روی کیبورد (مثل **Space**) را چندبار فشار دهیم.

PowerShell Error

اگر قصد نصب یک **Package** را داشته باشید، و مدام با خطایی مشابه زیر مواجه می شویم:

WARNING: MSG:UnableToDownload «https://go.microsoft.com/fwlink/?LinkID=627338&clcid=0x409» «»
WARNING: Unable to download the list of available providers. Check your internet connection.
WARNING: Unable to download from URI 'https://go.microsoft.com/fwlink/?LinkID=627338&clcid=0x409' to ''.

1. سیستم را به اینترنت متصل کنید.
2. توسط دستور زیر، پروتکل های قابل پشتیبانی سیستم را مشاهده کنید:

```
[Net.ServicePointManager]::SecurityProtocol
```

3. توسط دستور زیر، کلیدهای **Registry** برای رمزنگاری سطح بالای مربوط به **.NET Framework 64bit** را تنظیم کنید:

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord
```

4. توسط دستور زیر، کلیدهای **Registry** برای رمزنگاری سطح بالای مربوط به **.NET Framework 32bit** را تنظیم کنید:

```
Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord
```

5. **PowerShell** را یکبار کاملاً بسته و دوباره باز کنید؛ حال می توانید دوباره پروتکلهای قابل پشتیبانی را مشاهده کنید.

Doesn't join to Domain: because the SID of the Domain zou attempted to join was…

در **cmd** توسط دستور **cd** به مسیر درایو ویندوز رفته و سپس به مسیر زیر رفته و فایل زیر را درج کرده و اینتر:

C:\Windows\system32\sysprep\sysprep.exe

و یا دستور زیر را وارد می کنیم:

%WINDIR%\system32\sysprep\sysprep.exe

گزینه ی اول را روی **Enter System Audit Mode** قرار داده و **Generalize** را فعال کرده و گزینه ی دوم را روی **Reboot** یا **Shutdown** قرار می دهیم و **OK**.

Unable to connect to the Remote Server

فرض کنید در DC01 و در DC02 سرویس IIS نصب شده باشد.

حال می خواهیم در کنسول IIS مربوط به DC1 به سرویس IIS مربوط به DC2 هم متصل شویم.

1. وارد کنسول IIS مربوط به DC1 شده و بر روی گزینه ی Start Page در کادر سمت چپ کلیک راست کرده و Connect to a Server را زده و نام Domain مربوط به DC2 را درج کرده و با مشخصات یک Admin User وارد می شویم.

- اگر خطای Unable to connect to the Remote Server را می دهد، یعنی باید قابلیت Remote Connection را روی DC02 فعال کنیم.
- پس یا وارد DC2 شده و یا یک Session به آن زده و دستور زیر را برای تنظیم Registry آن وارد می کنیم:

```
Set-ItemProperty -Path "HKLM:\Software\microsoft\webmanagement\server" -Name "EnableRemoteManagement" -Value 1
```

- حال سرویس Web Management را فعال می کنیم:

```
Set-Service wMSVC -StartupType Automatic
```

- سیستم DC2 را یکبار Restart کرده و Session را قطع می کنیم.
- دوباره امتحان می کنیم و Connect را زده و finish!

: Commands in Run (WIN + R)

appwiz.cpl	**Program and Features** را باز می کند.
calc.exe	ماشین حساب ویندوز را باز می کند.
certmgr.msc	کنسول **Certification Authority** را برای **User** جاری، باز می کند.
cmd	**command prompt** را باز می کند.
winver	نسخه ی دقیق **Windows** را نمایش می دهد.
compmgmt.msc	**Computer Management**را باز می کند.
control	**Control Panel** را باز می کند.
devmgmt.msc	**Device Manager** را باز می کند.
dhcpmgmt.msc	کنسول **DHCP** را باز می کند.
diskmgmt.msc	برای مدیریت دیسک ها، پارتیشن ها و ولوم ها.
dnsmgmt.msc	کنسول **DNS** را باز می کند.
domain.msc	**AD Domains and Trusts** را باز می کند.
dsa.msc	**AD Users and Computers** را باز می کند.
Dssite.msc	**AD Sites and Services** را باز می کند.
dxdiag	اطلاعات دقیق و کامل نرم افزارها و سخت افزارهای سیستم را نشان می دهد.
eventvwr	پنجره ی **Event Viewer** را باز می کند.
chromeیا وFirefox	برای باز کردن این نرم افزارهاست.
fsmgmt.msc	کنسول **Shared Folders** را باز می کند.
Gpedit.msc	برای باز کردن پنجره ی **Policy Group** می باشد.
gpmc.msc	کنسول **Policy Manager Group** را باز می کند.
hostname	نام **Computer** را می دهد
lusrmgr.msc	کنسول **Local Users and Groups** را باز می کند.
Msconfig	**System Configuration** : جهت مدیریت **Start up** بکار می رود را باز می کند.
msinfo32	پنجره ی **System Informations** : اطلاعات سخت افزاری سیستم
ms-settings:windowsupdate	پنجره ی **Windows Update** را باز می کند
mstsc	**Remote Desktop** را باز می کند.
ncpa.cpl	صفحه ی **Network Connection** را باز می کند.
netplwiz	برای مدیریت یوزرها و گروه هاست.
Regedit	**Registry Editor**را باز می کند.
rrasmgmt.msc	کنسول **Routing and Remote Access** را باز می کند.
services.msc	کنسول **Windows Services** را باز می کند.
shutdown -r -t 0	**PC**را **Restart** می کند
shutdown -s -t 0	**PC**را خاموش می کند
snippingtool	عکسبرداری کردن از محتویات صفحه
virtmgmt.msc	کنسول **HyperV** را باز می کند.
Cluadmin.msc	کنسول **Failover Cluster Manager** را باز می کند.

نکته: برای اینکه هریک از کنسول ها را توسط نوار Run، با دسترسی Admin باز کنیم، کافی ست به جای Enter، دکمه های Ctrl+Shift را بگیریم، و سپس Enter را بزنیم.

CMD for Network :

hostname	برای دیدن نام کامپیوتر جاری
Ping 8.8.8.8	تست اتصال به Google را چک می کند که برای تست اتصال اینترنت بکار می رود.
Ping -t x.x.x.x	تست پیوسته ی اتصال سیستم مورد نظر با چک و قطع و وصل کردن کابل ها و سوییچ ها
Ping -a x.x.x.x	اگر بخواهیم نام مربوط به یک IP را پیدا کنیم.
Ping [خود سیستم IP]	چک می کند که پروتکل TCP-IP به درستی روی سیستم local نصب شده و کار می کند.
ping localhost	
Pathping [x.x.x.x]	مشابه Ping است، اما Router های موجود تا مقصد را نشان می دهد.
Tracert [www.name.com]	گام ها و روترهایی که برای طی شدن بسته های درخواست و دریافت تا باز شدن یک وبسایت لازم است را نشان می دهد.
ipconfig /all	نمایش مشخصات تمام NIC ها همراه با جزییاتی مثل DHCP و DNS
Ping -n عدد [IP یا name]	به تعداد دلخواهی، به یک Name یا IP عمل Ping را انجام می دهد.
Ping 127.0.0.1	سلامت و برقرار بودن کارت شبکه خودمان را چک می کند.
Getmac /V	پیدا کردن Mac Address و همچنین نام کارت شبکه ی سیستم
arp -a	پیدا کردن Mac Address و IP همه ی دستگاه هایی که به سیستم متصل اند (ARP Table).
nslookup	نام Domain شبکه و Server IP شبکه را می دهد، و با درج خط فرمان، کاربر می تواند Name/IP هر عضو از شبکه ی داخلی و یا شبکه ی اینترنت (مثل وبسایت ها) را وارد کند تا Name/IP آن را نیز دریافت کند.
ncpa.cpl	پنجره ی Network Connection
Ipconfig /flushdns	زمانی که DNS جدید سِت می کنیم، Cache سرویس DNS تا آن لحظه را خالی می کند.
Net view <Name or IP>	نمایش لیست فایل های share شده در سیستم مقصد
Dcdiag	صحت ارتباط میان این DC با DC های دیگر را جهت replication تست می کند.
whoami	نشان می دهد که با چه User ای وارد شده اید.
whoami /fqdn	آدرس distinguished مربوط به User ای که با آن Log in کرده ایم را می دهد.
whoami /groups	نشان می دهد که User تان عضو چه گروه هایی است.
net accounts	برای دیدن تنظیمات پسورد User تان
nltest /dsgetsite	اعلام می کند که این سیستم عضو کدام Site در Active Directory است.
slmgr /dlv	مشاهده ی مشخصات Key Activation ویندوز
whoami	نام User کنونی را می دهد.

نکته : اگر firewall ویندوز فعال باشد، و یا در نرم افزار Antivirus، در بخش Network connection، گزینه ی Firewall فعال باشد، Ping شدن به سیستم ممکن نیست.

نکته : در حقیقت اگر Name یکی از اعضای شبکه را داشته باشیم و IP آن را بخواهیم، می توان با ping کردن به نام آن، به سادگی در اولین خطِ پاسخ، IP آن را مشاهده کرد.

نکته: اگر با ping کردن به یک Name، پاسخ را بصورت IPv6 دریافت کردیم، می توانیم دستور را به صورت زیر درج کنیم تا پاسخ را همراه با IPv4 دریافت کنیم:

Ping Name -v 4

به همین طریق به سادگی می توان IP وبسایت های اینترنتی را نیز بدست آورد.

برای ذخیره کردن نتایج یک دستور cmd ، به این شکل عمل می کنیم:

[نام دستور] > [نام دلخواه].txt

برای باز کردن فایل ذخیره شده، کافیست در RUN تایپ کنید:

[نام دلخواه].txt

Review of Tools and Services :

Tool / Service	Description
CSVDE	برای انتقال Object های AD (مثل User ها و OU ها و Computer ها و ...) از یک Domain به یک Domain دیگر
Deduplication	فضای موردنیاز برای ذخیره سازی فایل ها را کاهش می دهد.
Hosted BranchCache Server	وقتی قصد ارتباط با یک شبکه ی Remote را داریم، و اغلب نیاز به تبادل فایلهای سنگین است، Hosted BranchCache راه اندازی می کنیم. برای Web Server ها و File Server ها و Application Server ها استفاده می شود.
KMS - Volume Licensing	برای Activate کردن ویندوزهای Client های شبکه، توسط Serial Number گروهی : کافی ست که اعضا به این Server متصل شوند، خودکار فعال می شوند.
PowerShell DSC	برای نصب یک یا تعدادی Windows Feature در بیش از یک Server به طور همزمان و از راه دور
QOS	برای کنترل و حفظ سرعت در شبکه هایی که VoIP و Conference Video و تبادل های Big Data استفاده و انجام می شود.
QOS Modem	اگر کاربران در یک محیط، در استفاده از حجم اینترنت دچار مشکل و مناقشه شده باشند.می توان توسط این مودم یا سوییچ ها اولویت بندی ایجاد کرد.
Upgrade the AD	برای ارتقاء نسخه ی Windows سرور اصلی یا DC شبکه استفاده می شود.
WDS Server	برای Install ویندوزهای Client های شبکه همراه با Driver های موردنیاز، به صورت خودکار و همزمان
Windows Server Migration	برای انتقال یک DHCP Server یا DNS Server و یا هر Server ای که یک Service خاص را تحت نسخه ی قدیمی تری از Windows ارائه می دهد، به یک Windows با نسخه ی جدیدتر.
Quota Management	برای استفاده از پوشه ها، محدودیت فضایی ایجاد می کنیم.
WSUS Server	دریافت Update ها از سایت Microsoft و توزیع آنها میان Client ها و Server های دیگر

نوشته ی
پیام اوَروند
پاییز 2020 - 1399

Payam_Avar@yahoo.com
@payam.avarwand